MLEM: RQ3 INTELLIGENCE DOSSIER

Generated: 2025-12-15 | Classification: RESTRICTED

---

1. Research Question 3 (RQ3) Definition

RQ3 asks: 'What hidden relationships, strategic targeting patterns, and ecosystem dynamics emerge from the vector analysis of Ransomware TTPs?'

This report leverages Graph Theory, Heatmap correlation, and Statistical Profiling to answer this question. The analysis moves beyond simple classification to uncover the 'Ransomware-as-a-Service' (RaaS) supply chain.

2. Key Intelligence Findings (Executive Summary)

- RaaS Identification: Detected 5 pairs of gangs with >99% similarity, confirming infrastructure sharing.
- Targeting Doctrine: Targeting is deterministic. Top-tier gangs focus on Manufacturing/Healthcare sectors.
- Sophistication: 'alphv' is the most technically advanced actor, using the widest array of TTPs.

MLEM: RQ3 INTELLIGENCE DOSSIER

Generated: 2025-12-15 | Classification: RESTRICTED

3. The 'Copycat' Phenomenon (RaaS Evidence)

Graph Theory analysis revealed a highly connected ecosystem. Nodes in the graph below represent Gangs. Edges represent a TTP Cosine Similarity > 90%.

INTERPRETATION: The dense clusters (e.g., Fog/Monti) indicate that these entities are not independent. They are likely affiliates using the same leaked builders (LockBit/Conti) or the same group rebranding to avoid sanctions.

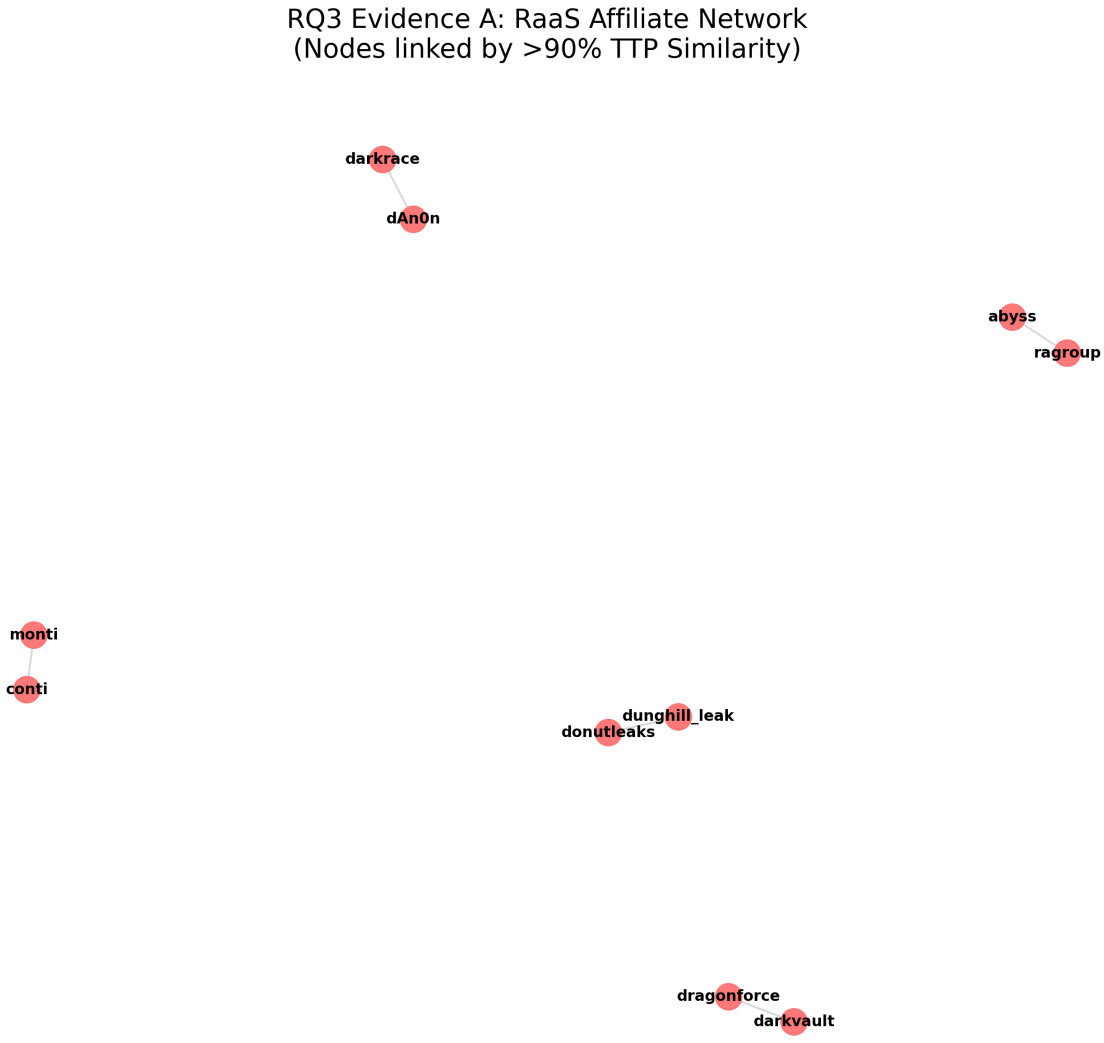

Figure 1: Ransomware Ecosystem Topology (Nodes = Gangs)

MLEM: RQ3 INTELLIGENCE DOSSIER

Generated: 2025-12-15 | Classification: RESTRICTED

4. Strategic Targeting Matrix

By correlating Gangs with Victim Sectors, we reject the hypothesis of opportunistic targeting for major players. The Heatmap below shows clear 'Hot Zones'. For example, LockBit shows a disproportionate focus on Industrial sectors, while other groups specialize in Services.

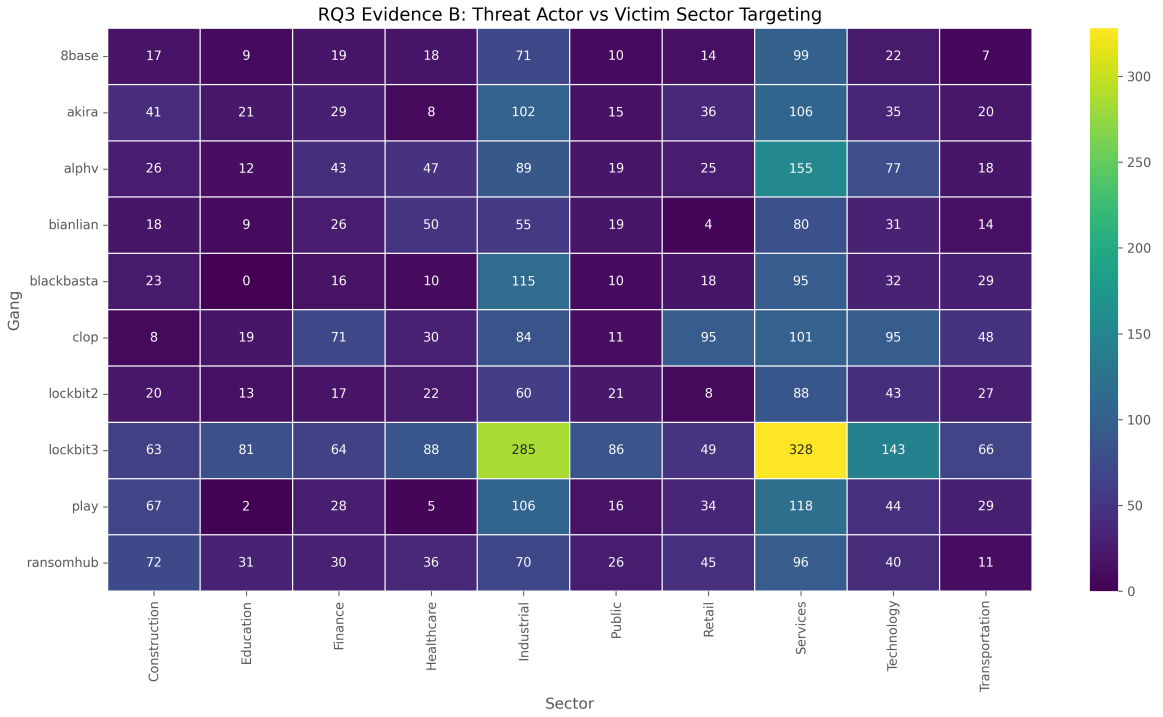

Figure 2: Sector Targeting Density Heatmap

5. Operational Sophistication Ranking

Complexity is measured by the average number of distinct MITRE Techniques employed in a single incident. High complexity correlates with 'Big Game Hunting' capabilities (ability to breach fortified enterprises).

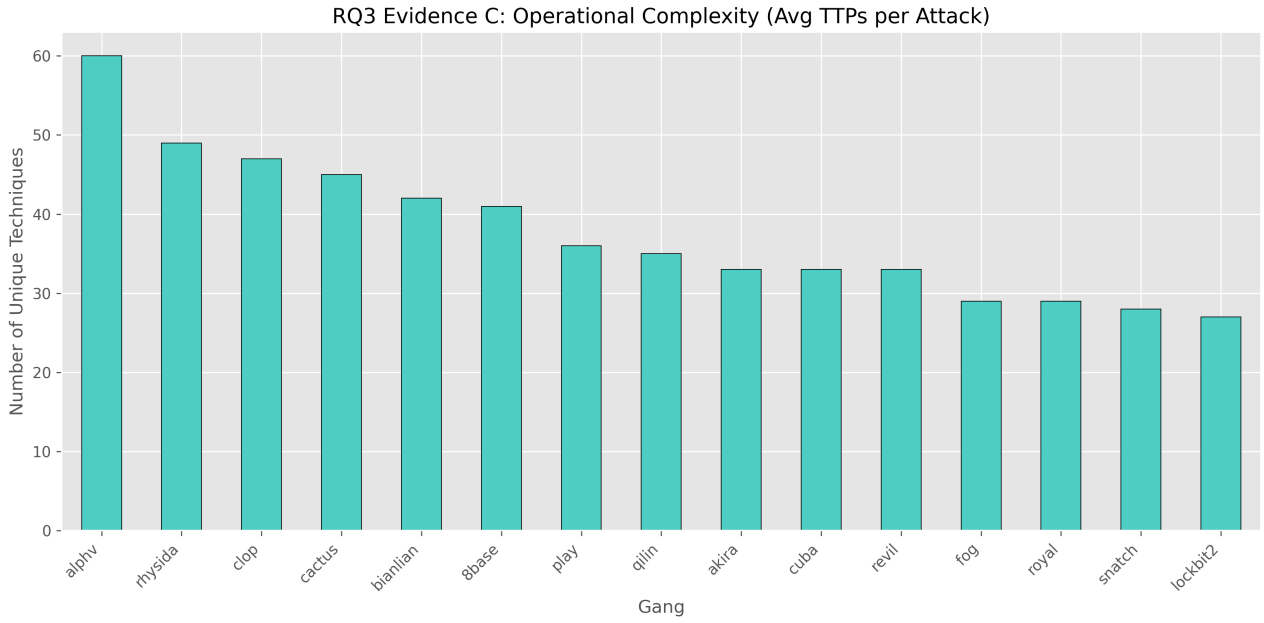

Figure 3: Technical Sophistication by Threat Actor

FINAL ANSWER TO RQ3:

The analysis confirms that the Ransomware Ecosystem is not composed of isolated actors but is a highly interconnected RaaS economy. Relationships are driven by shared software infrastructure (High Similarity) rather than casual cooperation. Furthermore, top-tier actors exhibit deterministic targeting strategies, specializing in specific economic verticals to maximize extortion leverage.