Ransomware Threats in Manufacturing: Patterns from Dark Web Tor Groups

Luis de-Marcos, Adrian Dominguez-Diaz
Carlos Cilleruelo, **Daniel Rodriguez**

Universidad de Alcalá, Spain

S2AIM 2025

Overview

- **Objective**: Analyze ransomware attacks on manufacturing using dark web data (April 2022–March 2025).
- **Dataset**: 7,427 ransomware attack records from Tor onion services.
- **Research Questions**:
  - RQ1: Vulnerability of manufacturing vs. other sectors.
  - RQ2: Geographic distribution of attacks.
  - RQ3: Diversity of ransomware groups.
  - RQ4: Temporal evolution of attacks.
- **Key Findings**: Manufacturing highly vulnerable, U.S. and Germany most affected, diverse groups, increasing trends.

Importance of Ransomware Threats in Manufacturing

- **Critical Impact**: Ransomware halts production, disrupts supply chains, and causes significant financial losses.
- **Industry 4.0 Risks**: IIoT and cyber-physical systems increase attack surfaces, exposing OT/ICS vulnerabilities.
- **Intellectual Property Theft**: Stolen designs and proprietary data threaten competitive advantage.
- **Economic and Safety Concerns**: Downtime affects global markets; compromised systems risk operational safety.
- **Urgent Need**: Tailored cybersecurity (e.g., network segmentation, real-time detection) to protect manufacturing.

Introduction

- Manufacturing’s reliance on Industry 4.0 increases cyber risks.
- Ransomware disrupts operations and compromises intellectual property.
- Dark web platforms provide insights into attack disclosures.
- Gap: Limited use of dark web data to study manufacturing threats.
- Study analyzes 7,427 attack records to address this gap.

Methods: Data Collection

- **Source**: 10,000 ransomware attack records from Tor groups (e.g., Akira, BianLian).
- **Period**: April 2022–March 2025.
- **Record Fields**: Group, company name, website URL, country code, disclosure date, NAICS code.
- **Collection**: Byron Labs scraped victim data from ransomware blogs.

Methods: Data Cleaning and NAICS Mapping

- **Initial Dataset**: 10,000 records.
- **Cleaning Steps**:
  - Removed duplicates: 8,511 records.
  - Excluded 181 records with missing country data.
  - Inferred NAICS codes using Claude 3.5 Sonnet (81% accuracy).
  - Removed 1,084 records with unassignable NAICS codes.
- **Final Dataset**: 7,427 records.
- **NAICS Mapping**: Codes 31–33 (Manufacturing), 44–45 (Retail), 48–49 (Transportation).

Results: RQ1 - Sector Vulnerability

- Manufacturing (NAICS 31–33) tied with Professional Services: 1,620 attacks each (21.81%).
- Other sectors: Retail Trade (6.05%), Education (5.98%), Healthcare (5.26%).
- Driven by OT reliance and downtime costs.

Code	Industry Sector	#Attacks	%
31–33	Manufacturing	1620	21.81
54	Professional Services	1620	21.81
44–45	Retail Trade	449	6.05
61	Educational Services	444	5.98
62	Healthcare	391	5.26

Results: RQ2 - Geographic Distribution

- **Top Countries (Manufacturing)**:
  - U.S.: 806 attacks (49.78%).
  - Germany: 115 attacks (7.10%).
  - U.K.: 58 attacks (3.58%).
- Germany's prominence reflects automotive/machinery sectors.

Rank #Attacks	Manufacturing	#Attacks	Overall
1 3970	U.S.	806	U.S.
2 394	Germany	115	U.K.
3 307	U.K.	58	Germany
4 251	Italy	57	Canada
5 234	Canada	50	France

Results: RQ3 - Ransomware Group Diversity

- 88 of 112 groups (78.57%) targeted manufacturing.
- **Top 5 Groups (51.85% of attacks)**:
  - **LockBit**: 363 attacks (22.41%); uses double-extortion, targets OT/ICS.
  - **Play**: 170 attacks; focuses on data leaks, rapid attacks.
  - **Black Basta**: 143 attacks; exploits supply chain vulnerabilities.
  - **ClOp**: 85 attacks; targets high-value firms, leaks data.
  - **Ransomhub**: 79 attacks; emerging group, aggressive extortion.

Results: RQ4 - Temporal Evolution

- **Annual Trends**:
  - 2022: 294 attacks (April–December).
  - 2023: 575 attacks (+95.58%).
  - 2024: 616 attacks (+7.13%).
  - 2025: 135 attacks (January–March).
- **Peaks**: June 2023 (87 attacks), March 2024 (73 attacks).
- Suggests increasing threat, possible decline in 2025.

Discussion: Vulnerability and Geography

- Manufacturing vulnerable due to OT/ICS and Industry 4.0 adoption.
- U.S. (49.78%) and Germany (7.10%) face concentrated attacks.
- Germany’s automotive and Asia’s electronics sectors targeted.
- Need for global collaboration and threat intelligence sharing.

Discussion: Groups and Trends

- Diverse groups (88/112) exploit legacy systems, supply chains.
- LockBit leads with double-extortion tactics.
- Attacks peaked in 2024, possible 2025 decline needs monitoring.
- Geopolitical factors may drive attack patterns.

Implications and Limitations

- **Implications**:
  - U.S./Germany: Enhance OT security, training, incident response.
  - Global: Share threat intelligence, regulatory frameworks.
  - Technical: Network segmentation, real-time detection.
- **Limitations**:
  - Dark web data may miss undisclosed attacks.
  - NAICS inference excluded 1,084 records.
  - 181 records lacked country data.

Future Work

- Integrate cybersecurity firm reports, company surveys.
- Analyze tactics of top groups (e.g., LockBit).
- Explore machine learning, blockchain for prevention.
- Study geopolitical influences on attack patterns.

Acknowledgements and Questions

- **Funding**: Project PID2021-125645OB-100 (PARCHE), MCIN/AEI/FEDER, EU.
- **Data Support**: ByronLabs S.L. for dark web tools and data.

Thank you! Questions?