

Ransomware Threats in Manufacturing Industry: Patterns based on Dark Web Telegram Groups

Luis De-Marcos
Department of Computer Science
Universidad de Alcalá
Alcalá de Henares, Spain
luis.demarcos@uah.es

Adrián Domínguez-Díaz
Department of Computer Science
Universidad de Alcalá
Alcalá de Henares, Spain
adrian.dominguez@uah.es

Carlos Cilleruelo
Department of Computer Science
Universidad de Alcalá
Alcalá de Henares, Spain
carlos.cilleruelo@uah.es

Daniel Rodríguez
Department of Computer Science
Universidad de Alcalá
Alcalá de Henares, Spain
daniel.rodriguezg@uah.es

Abstract— The manufacturing sector's increasing reliance on Industry 4.0 technologies has made it a prime target for ransomware attacks, which can disrupt operations, cause financial losses, and compromise intellectual property. While prior studies have explored ransomware threats to industrial systems, few have leveraged dark web-disclosed data to understand the scale and nature of these attacks. This study analyzes 7,427 ransomware attack records disclosed on dark web Telegram groups from April 2022 to March 2024, focusing on the manufacturing sector. The dataset, initially comprising 10,000 records, was cleaned by removing duplicates and records with missing NAICS codes, inferred using an AI-based approach. Findings reveal that manufacturing is vulnerable, with 1,620 attacks (21.81% of the total), tied with Professional Services as the most targeted sector. The United States accounted for 49.78% of manufacturing attacks, followed by Germany (7.10%), reflecting their significant manufacturing bases. A diverse set of 88 ransomware groups (78.57% of the total 112) targeted manufacturing, with LockBit responsible for 22.41% of attacks. These results underscore the urgent need for tailored cybersecurity strategies in manufacturing, including enhanced OT security and international collaboration to mitigate ransomware threats, particularly in high-risk regions like the U.S. and Germany.

Keywords—cyberattack, ransomware, manufacturing, dark web

I. INTRODUCTION

The rapid digitization of the manufacturing industry, driven by the adoption of Industry 4.0 technologies such as the Industrial Internet of Things (IIoT) and cyber-physical systems, has significantly enhanced operational efficiency and innovation. However, this digital transformation has also exposed the sector to escalating cybersecurity threats, with ransomware emerging as a particularly disruptive force [1], [2]. Ransomware attacks, which encrypt critical data or systems and demand payment for their release, pose a severe risk to manufacturing environments where operational continuity is paramount. The integration of operational technology (OT) and industrial control systems (ICS) in manufacturing has created unique vulnerabilities, as these systems are often ill-equipped to withstand sophisticated cyber threats, leading to potential production halts, financial losses, and intellectual property theft [3], [4].

Recent studies have underscored the growing prevalence of ransomware attacks targeting the manufacturing sector. For instance, research on IIoT systems has highlighted the evolving tactics of ransomware groups, emphasizing the urgent need for

advanced detection mechanisms to protect critical infrastructure [2]. Similarly, analyses of ransomware attacks on ICS in the oil and gas sector have revealed significant security challenges, advocating for enhanced measures like network segmentation and incident response plans [4]. The manufacturing industry's susceptibility is further compounded by the lack of real-time security solutions tailored to its operational constraints, as traditional cybersecurity tools often introduce system overhead or alert fatigue, hindering effective response [7]. Moreover, the complexity of predicting and detecting ransomware attacks on ICS necessitates a multidisciplinary approach, involving collaboration between cybersecurity experts and the ICS community [5], [9].

Specific ransomware groups, such as LockBit, have been identified as major threats to manufacturing, exploiting vulnerabilities in OT and ICS to maximize disruption [6]. Case studies of ransomware incidents in factories have provided valuable insights into attack patterns and digital forensic analysis, revealing the need for improved protective measures and legislative oversight to bolster resilience [8], [10], [11]. Despite these efforts, there remains a critical gap in the literature regarding the use of dark web-disclosed data to understand ransomware trends in manufacturing. Dark web platforms, such as Telegram groups, serve as a primary channel for ransomware groups to disclose attacks, leak stolen data, and negotiate ransoms, offering a unique window into the scale and nature of these threats. However, evidence leveraging such data to assess the impact on the manufacturing sector is scarce, limiting the industry's ability to develop targeted defenses.

This study addresses this gap by analyzing 7,427 ransomware attack records disclosed on dark web Telegram groups from April 2022 to March 2024, with a focus on the manufacturing sector. By examining this dataset, the study aims to provide a comprehensive understanding of ransomware threats to manufacturing, including their prevalence, geographic distribution, responsible actors, and temporal evolution. Specifically, the research seeks to answer the following questions:

RQ1: How Vulnerable is the Manufacturing Sector to Ransomware Attacks Compared to Other Industries?

RQ2: Which Countries are Most Affected by Ransomware Attacks on the Manufacturing Sector?

RQ3: What is the Role of Ransomware Group Diversity in Targeting the Manufacturing Sector?

RQ4: How Have Ransomware Attacks on the Manufacturing Sector Evolved Over the Period from April 2022 to March 2024?

II. METHODS

This study investigates the impact of ransomware attacks on the manufacturing sector using data disclosed on dark web Telegram groups. The methodology encompasses data collection, cleaning, preprocessing, and analysis, with a focus on ensuring the dataset's reliability for addressing the research questions.

The initial dataset consists of 10,000 records of ransomware attacks disclosed on dark web Telegram groups, covering the period from April 2022 to March 2025. Each record represents a unique ransomware attack and includes: the group disclosing the attack, the name of the targeted company, a URL linking to the company's website, country code of the company (e.g., US, DE), the date the attack was disclosed, and the NAICS code of the company, representing its industry classification. The dataset was collected from public disclosures on Telegram groups known for sharing ransomware attack information, providing a unique perspective on cybercriminal activity.

To ensure the dataset's quality, several cleaning and preprocessing steps were applied. First, duplicate records were removed, as some attacks were disclosed multiple times by the same or different groups. This process reduced the dataset from 10,000 to 8,511 records. All remaining records were verified to contain either the company name, the company link, or both, ensuring that each record could be associated with a specific entity. Next, records with missing country data were identified. Out of the 8,511 records, 181 lacked country information. These records were retained for analyses not requiring geographic data but were excluded from country-specific analyses to avoid bias.

The NAICS codes and corresponding industry information were not directly available in the raw dataset and required inference. The accuracy of this task was evaluated using three different LLMs: Claude 3.5 Sonnet, Claude 3 and AWS Titan. The models were asked to infer NAICS codes by conducting internet searches based on the company name and website. They retrieved relevant industry information and mapped it to the appropriate NAICS code. The evaluation was conducted on a sample of 42 manually labeled records. Claude 3.5 Sonnet achieved the highest accuracy (81%) and was used to populate the NAICS code field of each dataset record. Despite this effort, 1,084 records could not be assigned a NAICS code due to insufficient or ambiguous company information. These records were removed from the dataset, as industry classification was critical to the study's objectives. This final cleaning step resulted in a dataset of 7,427 records, which was used for all subsequent analyses.

To facilitate analysis, the industryCode column, representing the first two digits of the NAICS code, was processed to map specific ranges to their corresponding broad industry sectors. Codes 31, 32, and 33 were mapped to the "31-33" range (Manufacturing), 44 and 45 to "44-45" (Retail Trade), and 48 and 49 to "48-49" (Transportation and Warehousing). This

mapping ensured consistency with the NAICS classification system and enabled sector-level analysis.

III. RESULTS

To assess the vulnerability of the manufacturing sector to ransomware attacks, the distribution of attacks across industry sectors was examined. Table 1 shows the number of records and the percentage of total attacks for each broad industry sector, based on the NAICS industry codes.

TABLE I. DISTRIBUTION OF RANSOMWARE ATTACKS BY INDUSTRY SECTOR

Code	Industry Sector	#Attacks	%
11	Agriculture, Forestry, Fishing and Hunting	33	0.44
21	Mining, Quarrying, and Oil and Gas Extract.	55	0.74
22	Utilities	69	0.93
23	Construction	311	4.19
31-33	Manufacturing	1620	21.81
42	Wholesale Trade	370	4.98
44-45	Retail Trade	449	6.05
48-49	Transportation and Warehousing	231	3.11
51	Information	385	5.18
52	Finance and Insurance	356	4.79
53	Real Estate and Rental and Leasing	169	2.28
54	Professional, Scientific, and Technical Serv.	1620	21.81
55	Management of Companies and Enterprises	31	0.42
56	Administrative and Support Services	204	2.75
61	Educational Services	444	5.98
62	Health Care and Social Assistance	391	5.26
71	Arts, Entertainment, and Recreation	97	1.31
72	Accommodation and Food Services	158	2.13
81	Other Services (except Public Administration)	163	2.19
92	Public Administration	271	3.65

The manufacturing sector (NAICS 31-33) was one of the most targeted industries, with 1,620 records, accounting for 21.81% of all attacks. This is tied with the Professional, Scientific, and Technical Services sector (NAICS 54), which also recorded 1,620 attacks (21.81%). Other notable sectors include Retail Trade (6.05%), Educational Services (5.98%), and Health Care and Social Assistance (5.26%). The least targeted sectors were Management of Companies and Enterprises (0.42%) and Agriculture, Forestry, Fishing and Hunting (0.44%). These findings indicate that the manufacturing sector is highly vulnerable to ransomware attacks, likely due to its reliance on operational technology and the significant financial impact of production downtime.

The geographic distribution of ransomware attacks on the manufacturing sector was analyzed by identifying the top 10 countries with the most attacks. Out of 1,620 manufacturing records, 1,619 had valid country data. Table 2 compares the top 10 countries for manufacturing-specific attacks with the overall distribution of attacks across all sectors.

TABLE II. TOP 10 COUNTRIES FOR RANSOMWARE ATTACKS (MANUFACTURING VS. OVERALL)

Rank	Manufacturing	#Attacks	Overall	#Attacks
1	US	806	US	3970
2	DE (Germany)	115	GB (United Kingdom)	394
3	GB (United Kingdom)	58	DE (Germany)	307
4	IT (Italy)	57	CA (Canada)	251
5	CA (Canada)	50	FR (France)	234
6	JP (Japan)	49	IT (Italy)	197
7	FR (France)	41	BR (Brazil)	154
8	TW (Taiwan)	35	AU (Australia)	151
9	IN (India)	34	ES (Spain)	134
10	CN (China)	32	IN (India)	133

The United States was the most affected country for manufacturing attacks, with 806 records, representing 49.78% of all manufacturing attacks with country data. Germany followed with 115 attacks (7.10%), and the United Kingdom with 58 attacks (3.58%). Comparing this to the overall distribution, the U.S. also dominates with 3,970 attacks (53.45% of the total), but Germany's prominence in manufacturing attacks (115 out of 307 total attacks, or 37.46% of its attacks) highlights its significant manufacturing sector, likely in industries like automotive and machinery. Notably, countries like Japan (JP), Taiwan (TW), and China (CN) appear in the manufacturing top 10 but not in the overall top 10, reflecting their strong manufacturing bases, particularly in electronics and technology.

The diversity of ransomware groups targeting the manufacturing sector was examined to understand the breadth of actors involved. Across all sectors, 112 unique ransomware groups were identified. Of these, 88 groups (78.57%) targeted the manufacturing sector, indicating that manufacturing is a common target for a wide range of actors. The top five ransomware groups targeting manufacturing were responsible for a significant portion of attacks: LockBit (363 attacks), Play (170), Black Basta (143), Cl0p (85), Ransomhub (79). These five groups alone accounted for 840 attacks, or 51.85% of the 1,620 manufacturing attacks. LockBit was the most active, responsible for 22.41% of manufacturing attacks, suggesting that certain groups may specialize in targeting this sector due to its vulnerabilities, such as the potential for operational disruption and high ransom payouts.

The temporal evolution of ransomware attacks on the manufacturing sector was analyzed by examining the number of attacks per month and year. The dataset covers April 2022 to March 2024, with some additional records extending into 2025 (likely due to disclosure delays). We summarize the annual trends as follows: 294 during 2022, 575 during 2023, 616 in 2024, and 135 in 2025. Since the original data does not include complete accounts of 2022 and 2025, a monthly breakdown was also analyzed to identify patterns. The number of attacks on the manufacturing sector increased significantly over the study period, from 294 in 2022 (April to December) to 575 in 2023, a 95.58% increase. This trend continued into 2024, with 616 attacks, a further 7.13% increase from 2023. The 135 attacks in 2025 (January to March) reflect only a partial year but suggest a potential decline. Monthly data revealed peaks in June 2023 (87 attacks), July 2023 (76 attacks), and March 2024 (73 attacks),

possibly corresponding to periods of heightened ransomware activity or vulnerabilities in manufacturing operations. Conversely, lower activity was observed in April 2022 (15 attacks) and January 2023 (19 attacks), indicating variability in attack frequency over time.

IV. DISCUSSION

This study provides a comprehensive analysis of ransomware attacks on the manufacturing sector using dark web-disclosed data from April 2022 to March 2024. The findings offer critical insights into the sector's vulnerability, geographic distribution, ransomware group diversity, and temporal trends, addressing the four research questions and contributing to the broader understanding of cybersecurity threats in manufacturing.

The results indicate that the manufacturing sector (NAICS 31-33) is highly vulnerable to ransomware attacks, with 1,620 attacks accounting for 21.81% of the total 7,427 records, tied with Professional, Scientific, and Technical Services. This aligns with prior research highlighting manufacturing's susceptibility due to its reliance on OT and ICS, where downtime can lead to significant financial losses [2], [4]. The sector's vulnerability is likely exacerbated by the integration of Industry 4.0 technologies, which, while enhancing efficiency, introduce new attack vectors such as the Industrial Internet of Things (IIoT) [2]. Unlike sectors like Healthcare (5.26%) or Education (5.98%), where data breaches may target sensitive information, manufacturing attacks often aim to disrupt production, as noted in studies of ICS-targeted ransomware [5], [9]. This operational focus underscores the need for tailored cybersecurity measures, such as network segmentation and real-time detection systems, to mitigate the impact of ransomware on manufacturing [4], [7].

The geographic analysis reveals that the United States is the most affected country, with 806 manufacturing attacks (49.78% of the sector's total), followed by Germany (115 attacks, 7.10%). This distribution mirrors the overall trend, where the U.S. accounts for 53.45% of all attacks, but Germany's prominence in manufacturing attacks (37.46% of its total attacks) reflects its significant manufacturing base, particularly in automotive and machinery sectors. Countries like Japan, Taiwan, and China, which appear in the manufacturing top 10 but not the overall top 10, are known for electronics manufacturing, suggesting that ransomware groups target regions with high concentrations of specific industries [8]. These findings highlight the need for international collaboration in cybersecurity, especially in high-risk regions like the U.S. and Germany, where manufacturing firms may benefit from shared threat intelligence and regulatory frameworks to bolster resilience [1], [11].

The diversity of ransomware groups targeting manufacturing is notable, with 88 out of 112 groups (78.57%) involved, and LockBit leading with 363 attacks (22.41% of manufacturing attacks). This high diversity indicates that manufacturing is a lucrative target for a wide range of actors, not just a few dominant groups, as supported by studies on ransomware tactics in industrial environments [6], [10]. LockBit's prominence aligns with prior research identifying it as a major threat to OT and ICS in manufacturing, often using double-extortion tactics

to maximize impact [6]. The involvement of groups like Play and Black Basta further suggests that manufacturing's vulnerabilities—such as legacy systems and interconnected supply chains—are exploited by multiple actors [8]. This diversity poses a challenge for defense strategies, as firms must prepare for varied attack methods, necessitating advanced detection systems like CanCal, which address system overhead and alert fatigue in industrial settings [7].

The temporal analysis shows an increase in ransomware attacks on manufacturing. Peaks in June 2023 (87 attacks) and March 2024 (73 attacks) may correspond to periods of heightened ransomware activity, possibly driven by geopolitical tensions or supply chain disruptions, as noted in prior studies [11]. The upward trend aligns with the evolving threat landscape described in the literature, where ransomware groups have increasingly targeted critical infrastructure like manufacturing to exploit operational dependencies [2], [5]. The slight decline in early 2025 (135 attacks) could indicate improved cybersecurity measures or a shift in attacker focus, but the partial year data limits definitive conclusions. These findings emphasize the need for continuous monitoring and adaptive security strategies to address the dynamic nature of ransomware threats [3].

A. Implications and Limitations

The high vulnerability and geographic concentration of attacks in the U.S. and Germany suggest that firms in these regions should prioritize OT security, employee training, and incident response plans, as recommended by prior research [1], [4]. The diversity of ransomware groups underscores the importance of developing versatile detection and mitigation strategies, potentially leveraging machine learning and blockchain technologies for real-time protection [3], [7]. The temporal increase in attacks highlights the urgency of proactive measures, such as early detection systems, to predict and prevent ransomware incidents [5], [9].

However, the study has limitations. The reliance on dark web-disclosed data may introduce bias, as not all attacks are publicly disclosed, and some disclosures may be delayed or incomplete. The inference of NAICS codes using AI, while effective for most records, resulted in the exclusion of 1,084 records, potentially underrepresenting certain industries. Additionally, 181 records lacked country data, which may skew the geographic analysis, particularly for smaller countries. Finally, the dataset's focus on disclosed attacks may not capture the full scope of ransomware incidents, as some firms may pay ransoms without public disclosure.

Future research should address these limitations by integrating additional data sources, such as incident reports from cybersecurity firms or direct surveys of manufacturing companies, to provide a more comprehensive view of ransomware threats. Exploring the specific tactics of top ransomware groups like LockBit in targeting manufacturing could inform more targeted defenses [6]. Additionally, investigating the effectiveness of emerging technologies, such

as incremental machine learning and blockchain, in preventing ransomware attacks on manufacturing systems could enhance real-time security [3]. Finally, a deeper analysis of temporal trends, including the impact of geopolitical events on attack patterns, could provide further insights into the evolving ransomware landscape [11].

Acknowledgements

The publication is part of the project PID2021-125645OB-I00 (PARCHE), funded by MCIN/AEI/10.13039/501100011033/FEDER, EU

ByronLabs S.L. supported this work by providing the tools to crawl the Dark Web and the raw data used in this study.

References

- [1] B. Fteiha, A. A. Ayoub, L. Y. Hussein, and H. Zia, "Securing the Future of Digital Manufacturing: A Review of Vulnerabilities and Mitigation Strategies," in *Proc. 5th Int. Conf. Commun., Inf., Electron. Energy Syst. (CIEES)*, Veliko Tarnovo, Bulgaria, 2024, pp. 1–8, doi: 10.1109/CIEES62939.2024.10811264.
- [2] M. Al-Hawawreh, M. Alazab, M. A. Ferrag, and M. Hossain, "Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms," *J. Netw. Comput. Appl.*, vol. 220, p. 103809, 2023, doi: 10.1016/j.jnca.2023.103809.
- [3] B. Oskolkov, K. Chen, W. Tian, A. C. C. Law, and C. Liu, "Incremental Machine Learning-integrated Blockchain for Real-time Security Protection in Cyber-enabled Manufacturing Systems," *J. Comput. Inf. Sci. Eng.*, pp. 1–27, 2025, doi: 10.1115/1.4067736.
- [4] T. Y. Elete, "Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations," *Comput. Sci. IT Res. J.*, vol. 5, no. 12, pp. 2664–2681, 2024, doi: 10.51594/csitrj.v5i12.1759.
- [5] M. Gazzan and F. T. Sheldon, "Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems," *Future Internet*, vol. 15, no. 4, p. 144, 2023, doi: 10.3390/fi15040144.
- [6] N. Suk-On, N. Thiratitsakun, and K. Chimmanee, "Digital Forensic Analysis of Lockbit Ransomware Attack on Operational Technology," in *Proc. Int. Conf. Innov. Comput., Inf. Technol. (INCIT)*, Nov. 2024, pp. 624–629, doi: 10.1109/incit63192.2024.10810564.
- [7] S. Wang, F. Dong, H. Yang, J. Xu, and H. Wang, "CanCal: Towards Real-time and Lightweight Ransomware Detection and Response in Industrial Environments," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS '24)*, New York, NY, USA, 2024, pp. 2326–2340, doi: 10.1145/3658644.3690269.
- [8] D. Liu, Y. Liu, Z. Liu, X. Zhang, and X. Zhang, "Analysis and Reflection on the Situation of Industrial Information Security Ransomware Attacks," in *Proc. 8th Int. Conf. Data Sci. Cyberspace (DSC)*, Aug. 2023, pp. 354–358, doi: 10.1109/dsc59305.2023.00057.
- [9] M. Gazzan and F. T. Sheldon, "Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems," *Future Internet*, vol. 15, no. 4, p. 144, 2023, doi: 10.3390/fi15040144.
- [10] P. Nakhonthai and K. Chimmanee, "Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories," in *Proc. 6th Int. Conf. Inf. Technol. (IncIT)*, Nonthaburi, Thailand, 2022, pp. 416–421, doi: 10.1109/InCIT56086.2022.10067356.
- [11] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet Things Cyber-Phys. Syst.*, 2024, doi: 10.1016/j.iotcps.2023.12.001.