ZEROFOX INTELLIGENCE

Brief

Ransomware and Government-Protected Manufacturing Jobs

B-2025-10-09c

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical

October 9, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 4:00 PM (EDT) on October 8, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | Ransomware and Government-Protected Manufacturing Jobs

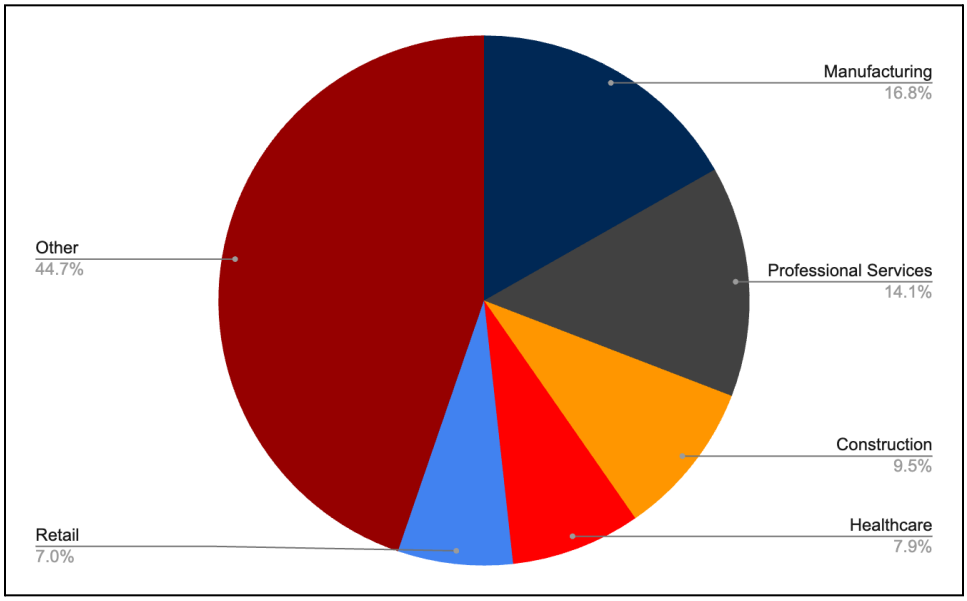
| Executive Summary

The ZeroFox Q3 Ransomware report found that the manufacturing sector was once again the most popular target for ransomware and digital extortion (R&DE) attacks, with the United States and Europe the most popular locations for attacks. This is despite the sector making up a decreasing share of economic output in those regions, as manufacturing jobs have shifted to Asia. The sector's low tolerance for downtime, complex supply chains, reliance on third-party vendors, and digitization of work sites are likely behind the rise. However, there is a roughly even chance that U.S. and European prioritization of the sector—via tariffs to specifically protect domestic manufacturing jobs or government bailouts to domestic manufacturing firms affected by cyber intrusions—is incentivizing threat actors.

Trends

In Q3 2025, North America-based organizations were the most targeted by a substantial margin, accounting for approximately 59 percent of all R&DE incidents. Europe-based organizations were the second most targeted region in Q3 2025, accounting for nearly 22 percent of all incidents. Together, North America and Europe-based organizations accounted for 81 percent of all R&DE incidents observed during Q3 2025, which is largely consistent with other quarters.

In Q3 2025, nearly 17 percent of all incidents targeted entities in the manufacturing sector. Manufacturing has consistently been the most targeted industry since at least 2021.[1]



Most heavily targeted industries in Q3 2025

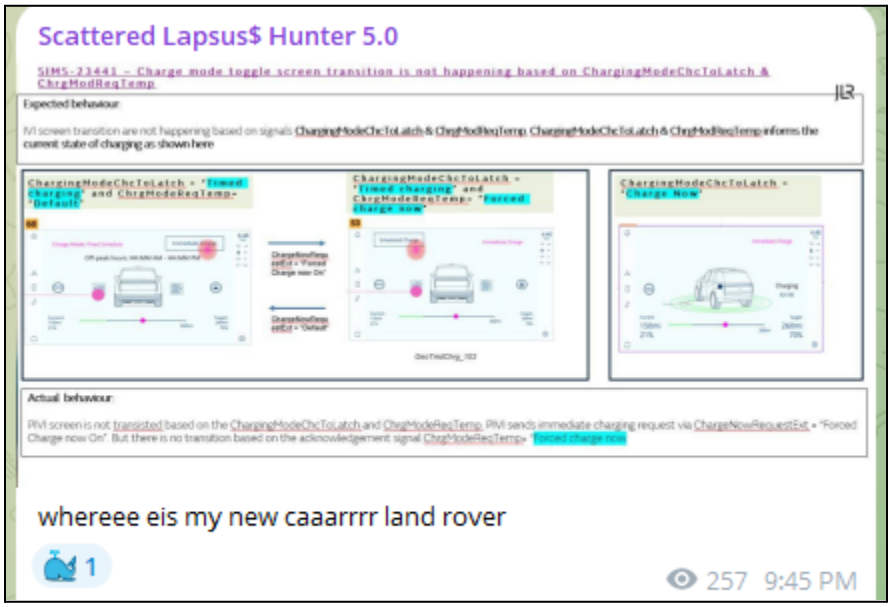
Source: ZeroFox Intelligence

High-Profile Incidents

There have been a number of recent high-profile R&DE incidents involving the sector led by the August 31 attack on UK-based automotive manufacturer Jaguar Land Rover (JLR) claimed by threat actor group "Scattered Lapsus$ Hunters" on its Telegram channel.

[1] ZeroFox Intelligence Assessment: Q3 2025 Ransomware Wrap-Up, October 3, 2025

- As proof of the compromise, Scattered Lapsus$ Hunters shared a screenshot from a command-line interface on JLR's network. Then on September 18, the group offered to sell data associated with multiple global organizations, including Jaguar, on its official Telegram channel.[2]
- JLR was forced to shut down its factories for over five weeks as part of efforts to contain the attack. Notably, the UK government agreed to guarantee JLR a USD 2 billion loan to ensure JLR could pay its suppliers and afford operating costs.[3]



Alleged JLR command-line interface posted on the Scattered Lapsus$ Hunters Telegram page
Source: hXXps://t[.]me/+FInBlpGYJIA2NTQ9

On October 7, French-based auto company Renault said UK customer data was stolen in a cyberattack targeting one of its data processing providers.[4] In September 2025, tire manufacturing company Bridgestone Americas was hit by an attack that halted production,[5] while European vehicle maker Stellantis recently reported the theft of U.S.

[2] ZeroFox Intelligence
[3] hXXps://www.itv[.]com/news/2025-09-27/government-to-back-huge-loan-to-jlr-in-order-to-save-supply-chain
[4] hXXps://www.computing[.]co[.]uk/news/2025/security/renault-notifies-customers-of-data-breach-linked-to-third-party-supplier
[5] hXXps://www.cybersecuritydive[.]com/news/bridgestone-americas-restores-facilities-network-connections-following-cyb/760381/

customer data in an attack against a third-party data platform according to a company statement on September 21.[6]

Analyst Commentary

ZeroFox assesses that the disproportionate targeting of Western entities can be partly attributed to the geopolitical motivations and ideological beliefs of financially motivated threat collectives fueled by opposition to "Western" political and social narratives. Furthermore, the manufacturing industry—wherein delays in manufacturing equate to lost sales and there is increasing use of vulnerable operational technology infrastructure behind automation efforts—has a low operational tolerance for downtime, particularly at smart factories that build vehicles such as Jaguar.

However, the manufacturing sector in both Europe and the United States has been shrinking for years. It makes up a decreasing share of the economic output of the United States and most European countries—including in the United Kingdom, where the auto industry is half the size it was in 2016.[7] On the other hand, manufacturing has been growing in Asia, where less than 9 percent of R&DE incidents took place in Q3 2025.[8]

Western States Prioritize Protecting the Manufacturing Sector

There is a roughly even chance the move by the UK government to loan JLR USD 2 billion could incite future attacks—even more so if companies opt to forego cybersecurity protections knowing the government will bail them out. However, the UK decision is just part of a wider pattern by the U.S. and European states to protect their domestic manufacturing sectors.

Protecting manufacturing jobs is a key justification for U.S. tariff policy in 2025. U.S. President Donald Trump has claimed that tariffs will protect U.S. manufacturers whose products would otherwise be uncompetitive compared to cheaper (mainly Asian)

[6] hXXps://media.stellantisnorthamerica[.]com/newsrelease.do
[7] hXXps://www.bloomberg[.]com/news/articles/2025-10-07/jaguar-land-rover-cyber-attack-why-uk-bailout-is-high-risk-move
[8] ZeroFox Intelligence Assessment: Q3 2025 Ransomware Wrap-Up, October 3, 2025

imports. For example, in June 2025, the Commerce Department announced 50 percent tariffs on imported steel, specifically to protect U.S. steelmakers from cheaper foreign competition.[9]

- The United States has also placed on-and-off tariffs targeting the auto sector, with the latest 25 percent tariffs on imported trucks going into effect on November 1, 2025.[10]
- Tariffs on furniture and lumber are designed to protect U.S. homebuilders and furniture makers,[11] while much of the commentary surrounding tariffs on China and other Asian manufacturing countries is focused on protecting manufacturing jobs.

On October 7, 2025, the European Commission unveiled a proposal to increase tariffs on steel imports from 25 to 50 percent and cut the volume of steel that is allowed into the European Union (EU) before that higher rate goes into effect.[12]

- By bringing its steel tariff rates in line with U.S. steel tariffs, the EU is likely indicating a broader approach to mirror U.S. tariff levels to ensure that cheaper (mainly Asian) imports no longer being exported to the United States do not make their way to Europe instead. Furthermore, these measures signify how likely the EU is to move to protect its critical industries. Similar tariffs to protect the automobile, luxury goods, and agricultural sectors are likely to be levied in the face of cheaper Asian alternatives.

The UK government has not announced new tariffs, but, earlier in 2025, it moved to protect its domestic steelmaking sector by passing the Steel Industry (Special Measures) Act 2025, which granted it emergency powers to intervene in critical steel manufacturing operations. The UK decision came after Jingye Group, the Chinese company that

[9] hXXps://www.whitehouse[.]gov/presidential-actions/2025/06/adjusting-imports-of-aluminum-and-steel-into-the-united-states/
[10] hXXps://www.freightwaves[.]com/news/trump-to-impose-25-tariff-on-trucks-starting-nov-1
[11] hXXps://www.nytimes[.]com/2025/09/29/business/economy/tariffs-cabinets-furniture-lumber-trump.html
[12] hXXps://www.euronews[.]com/business/2025/10/07/european-commission-wields-protective-powers-to-shield-eu-steel

acquired British Steel in March 2020, was on the verge of shuttering operations due to substantial daily financial losses of GBP 700,000.[13]

- The closure of British Steel's Scunthorpe site would have resulted in the United Kingdom becoming the only major Western economy without primary steel production. While the United Kingdom could have continued importing steel—likely for cheaper than what it would have cost to produce from Scunthorpe—doing so would have left the sovereign state reliant on trade partners who could have curtailed supplies at any moment.

Going Forward

European politicians have been debating for years how to boost the competitiveness of European businesses, which are rapidly losing market share to cheaper imports. Stopping and reversing the decline in EU manufacturing is critical to boosting overall EU business competitiveness. The U.S. tariff strategy and recent UK government actions protecting the automobile and steel industries have similar underlying intentions. It is unclear whether these measures are driving cyber threat actors to target the sector, but it is apparent that Western governments have determined that protecting industrial jobs and profitability are long-term priorities.

[13] ZeroFox Intelligence Flash Report: British Steel Operational Disruption, April 18, 2025

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%