Food Ag-ISAC

FARM-TO-TABLE RANSOMWARE REALITIES

EXPLORING THE 2025 RANSOMWARE LANDSCAPE AND **INSIGHTS FOR 2026**

February 2026

ABOUT THE FOOD AND AG-ISAC

The Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) was built by industry for industry - providing threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share indicators so they can better protect themselves and manage risks to their companies and the sector.

TABLE OF CONTENTS

INTRODUCTION

The ransomware landscape is a dynamic ecosystem where threat actors constantly refine their breach and extortion tactics. To counter these evolving threats, the Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC) in conjunction with the IT-ISAC has maintained a comprehensive database of ransomware attacks since 2020. To date, 15,265+ ransomware incidents have been recorded through proprietary automation tools that aggregate data from public breach reports, RSS feeds, dark web leak sites, and internal threat intelligence.

The ransomware tracker database is a queryable resource accessible to Food and Ag-ISAC members and acts as a central hub for monitoring ransomware incidents. This joint effort allows members to analyze trends together, enhances all participants' capacity to remain informed, and bolsters the community's overall resilience against ransomware attacks. When the ISAC and its member companies identify significant and emerging ransomware groups and incidents, comprehensive Adversary Attack Playbooks are built for them. The over 330 playbooks provide in-depth analysis of the groups' tactics, techniques, and procedures (TTPs), equipping members with valuable intelligence to enhance their cybersecurity defenses.

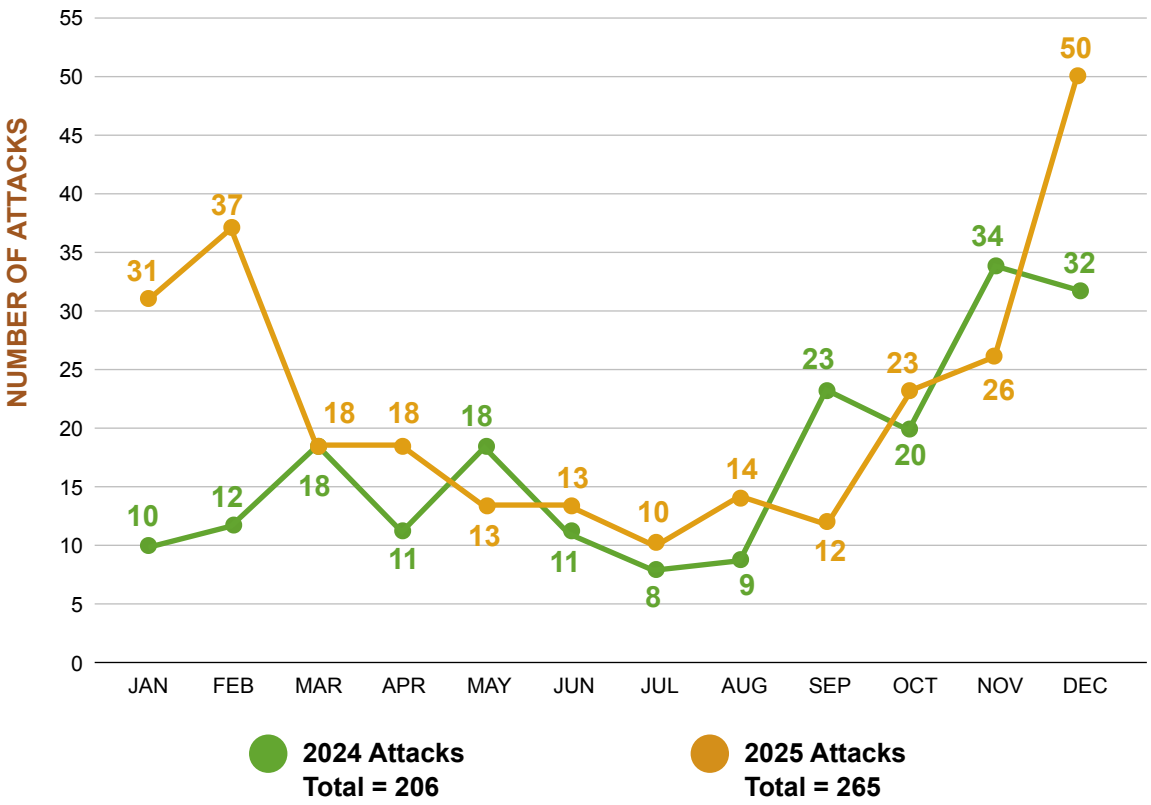
The Food and Ag-ISAC tracked approximately 6,377 ransomware incidents across all sectors in 2025, representing an 82% increase from the 3,508 incidents recorded in 2024. The steady increase over the years is attributable to both an improved ability to track ransomware attacks and a genuine escalation in ransomware operations. The ISAC continues to monitor attacks across multiple critical infrastructure sectors.

ATTACKS BY CRITICAL INFRASTRUCTURE

The food and agriculture sector was targeted by 265 attacks in 2025, which represented (4.2%) of the total ransomware volume across all critical sectors. While the attack rate was lower than in other sectors, the number of victims increased. Due to the sector's robust supply chain of many partners and suppliers, and the "just-in-time" delivery of products to consumers, ransomware attacks can be particularly damaging to the sector.

The number of ransomware attacks per month in 2024 and 2025 remained fairly consistent, with three notable exceptions. Attacks surged in January, February, and December 2025, the early-year spike driven primarily by CL0P's exploitation of a Cleo Managed File Transfer vulnerability. This campaign, which began in late 2024 and peaked in early 2025, affected multiple sectors beyond food and agriculture.

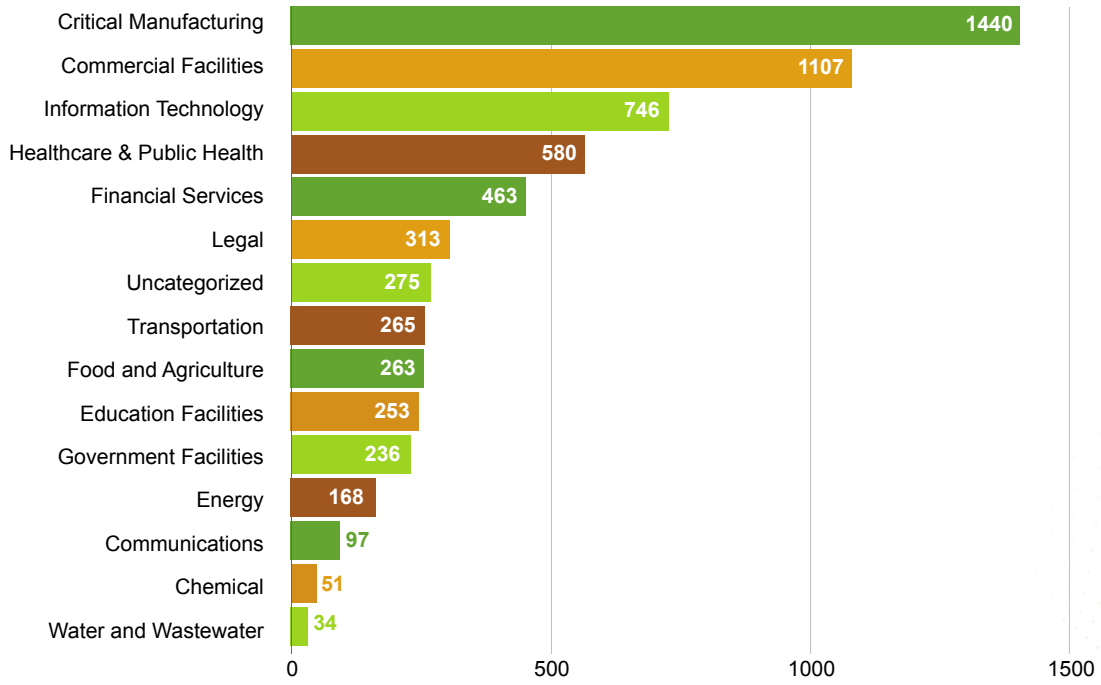
RANSOMWARE ATTACKS ON THE FOOD AND AG SECTOR 2024 VS 2025



To the right is a comparison of the food and agriculture sector with other sectors that ransomware actors targeted more prominently in 2025.

- The **critical manufacturing sector** saw the highest number of attacks we tracked, experiencing 1440 attacks (accounting for 22.7% of all incidents)
- Following closely, the **commercial facilities sector** saw 1107 attacks (17.5%)
- The information **technology sector** was affected by 746 attacks (11.8%)
- The **healthcare and public health sector** saw 580 attacks (9.2%)
- Additionally, the **financial services sector** experienced 463 attacks (7.3%)
- Finally, although not a critical infrastructure sector, it is worth noting that the **legal sector** accounted for 313 attacks (4.9%).

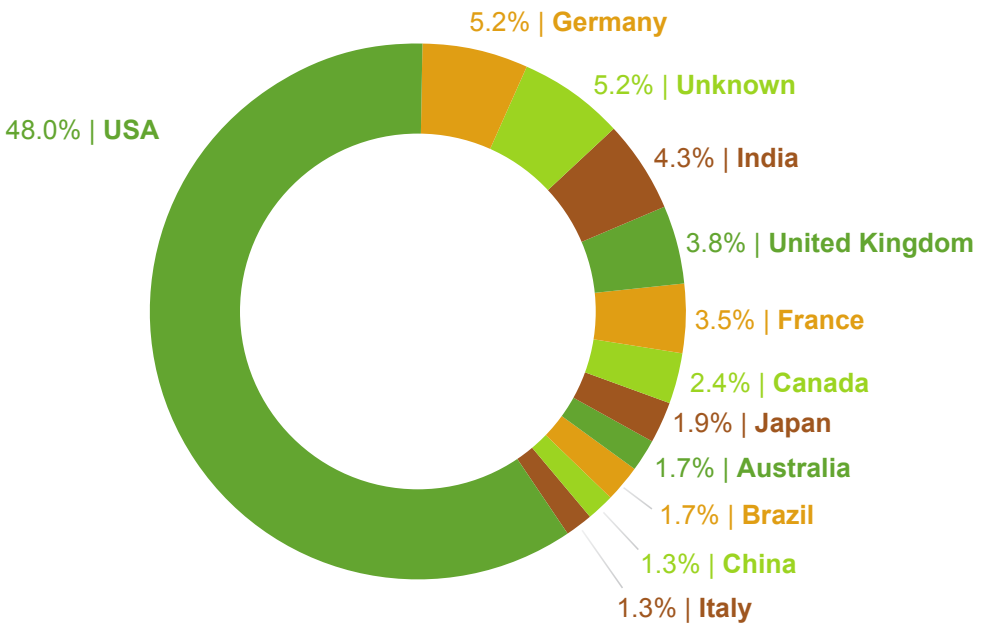
NUMBER OF ATTACKS ON CRITICAL INFRASTRUCTURE



ATTACKS BY COUNTRY

Ransomware activity concentrates heavily in the U.S., which experienced 3,311 attacks in 2025, over half (52.13%) of all global incidents. This volume highlights America's attractiveness as an economic and technological target. Every other country recorded fewer than 300 attacks, each accounting for less than 5% of the total. The U.S. remains a top-tier target for ransomware due to its economic scale and the critical nature of its corporate and public infrastructure. For threat actors, the country offers a high-reward environment where they can pursue both lucrative payouts and large-scale chaos.

NUMBER OF ATTACKS BY COUNTRY



This graph represents the top 12 countries attacked by ransomware groups in 2025.

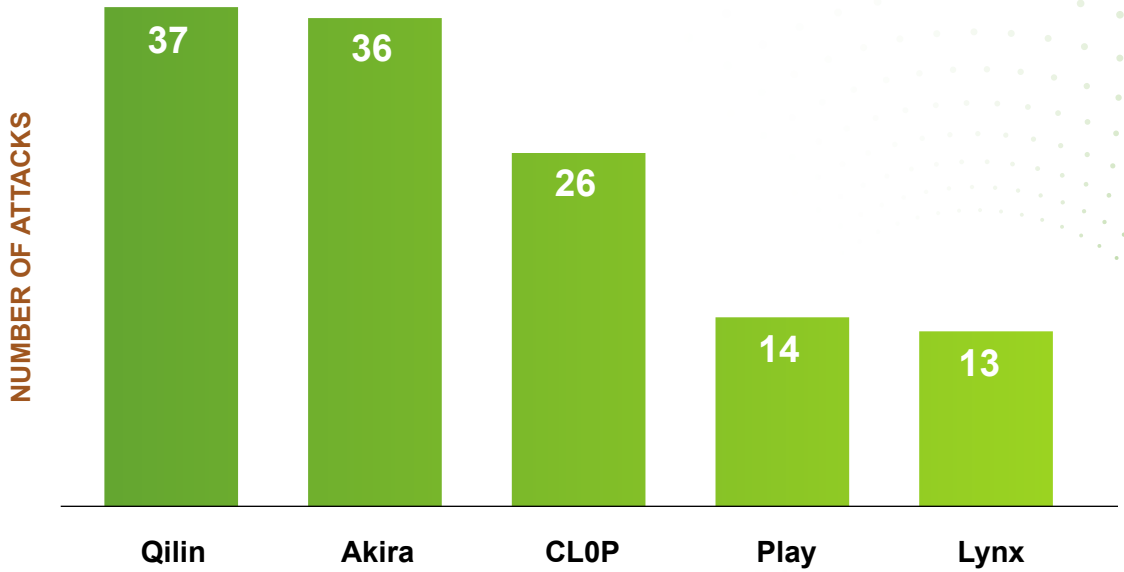
TOP 5 RANSOMWARE STRAINS | FOOD AND AG SECTOR

Five ransomware groups dominated attacks against the food and agriculture sector in 2025: Qilin, Akira, CL0P, Play, and Lynx. These actors accounted for nearly 50% of all ransomware incidents recorded by Food and Ag-ISAC, demonstrating their impact on the sector. Notably, three of these groups ranked among the top five threat actors across all critical infrastructure sectors - Qilin, Akira, INC Ransom, SafePay, and Play.

This generally indicates that threat actors largely are looking for victims of opportunity, rather than targeting the sector specifically. Opportunistic attacks scan for publicly exposed and vulnerable systems, purchase access from initial access brokers, and use phishing and social engineering tactics to target any vulnerable organization, regardless of its sector. Food and agriculture companies are inevitably targeted by ransomware attacks due to the sheer volume of indiscriminate attacks. However, CL0P is a notable outlier, suggesting a slight preference for the food and agriculture sector. We noted that CL0P attacked the food and agriculture sector in 9.3% of its attacks in 2025. This percentage was well ahead of the average targeting across all groups (4.2%)

Below includes a detailed look at the top five ransomware groups that targeted the food and agriculture sector in 2025.

TOP 5 RANSOMWARE ACTORS | FOOD AND AG SECTOR



EXPLOITED VULNERABILITIES

Overall, attacks observed in 2025 leveraged a wide range of initial access methods, including exploiting system and software vulnerabilities, employing social engineering tactics to deceive individuals into granting unauthorized access, and deploying malware to infiltrate and compromise victim networks. Below, we highlight some of the more significant vulnerabilities being exploited and common techniques used by ransomware attackers.

Citrix NetScaler

- CVE-2025-5777: Out-of-bounds Read (CVSS 9.3)

CrushFTP

- CVE-2025-31161: Critical Authentication Bypass

Fortinet

- CVE-2024-55591: Authentication Bypass (CWE-288)
- CVE-2025-24472: Authentication Bypass

GoAnywhere MFT

- CVE-2025-10035: Critical Deserialization of Untrusted Data (CVSS 10.0)

Ivanti Connect Secure

- CVE-2025-22457: Critical RCE (Stack-based Buffer Overflow)
- CVE-2025-0282: Critical RCE (Stack-based Buffer Overflow)
- CVE-2025-0283: Privilege Escalation

Microsoft SharePoint

- CVE-2025-53770 (“ToolShell”): Unauthenticated RCE via Deserialization (CVSS 9.8)
- CVE-2025-49704: Code Injection (Authorized)
- CVE-2025-49706: Improper Authentication

Mitel MiCollab

- CVE-2024-55550: Path Traversal

Oracle E-Business Suite

- CVE-2025-61884: Information Disclosure (Unauthenticated)

Redis

- CVE-2025-49844: Use-After-Free (RCE via Lua Sandbox Escape)

SonicWall

- CVE-2024-40766: Improper Access Control
- CVE-2025-40602: Missing Authorization

Windows Management Console (MMC)

- CVE-2025-26633: Security Feature Bypass

2026 PREDICTIONS

The ransomware threat landscape targeting food and agriculture continues to evolve rapidly, driven by fragmentation, technological innovation, and strategic adaptation by threat actors. Based on our research and analysis, we think the following four trends will shape the sector's risk profile in 2026, each amplifying vulnerabilities unique to food and agriculture operations.

- **Landscape of Smaller Ransomware Operations**
  As we enter 2026, the ransomware landscape appears to be moving away from traditional monolithic ransomware-as-a-service (RaaS) giants to smaller, more specialized ecosystems. The number of distinct ransomware groups surged in 2025, with estimates of a nearly 50% increase from the previous year. This number will grow further in 2026 as affiliates realize that smaller groups are harder for authorities to track.

  Groups now operate with shorter lifespans. Instead of building a multi-year brand, 2026 attackers prefer to launch a campaign, target a specific sector (such as manufacturing), and then dissolve or rebrand within months to evade sanctions and law enforcement.

- **The Return of Distributed-Denial-of-Service (DDoS) Attacks**
  Ransomware-as-a-service (RaaS) operations have returned to offering DDoS as a means to add additional pressure to victims and as a recruitment tool to affiliates. Attackers now layer a sustained DDoS attack on top of the initial breach. Even if the victim can restore their systems from backups, the DDoS attack keeps their website, customer portals, and APIs offline.

  Large remaining RaaS operators now bundle powerful DDoS botnets into their service offerings. Attackers can steal a small amount of sensitive data and then trigger a DDoS attack to force the victim to the negotiating table, or punish victims who are attempting to restore encrypted files.

- **Under the Visor**
  Attacking the underlying infrastructure (such as VMware ESXi or other hypervisors) remained a top trend in 2025, and one we expect to continue in 2026. By attacking the hypervisor, a single attack can take down hundreds of virtual machines at once. Ransomware groups are increasingly targeting the software-as-a-service (SaaS) providers that companies rely on. A single breach of a managed service provider (MSP) can now provide "automated access" to hundreds of victim networks.

- **Generative AI and Agentic AI**
  Adversaries will continue to leverage LLMs in 2026. Generative AI has improved the quality of phishing and social engineering attacks, and defending against these technologies will proliferate as LLMs and Deepfake technology continues to evolve. Initial access is increasingly achieved through hyper-realistic AI voice and video clones. An urgent call from a CEO, IT Director, or MSP help desk is now a primary way to bypass multi-factor authentication (MFA).

These converging trends create a more complex threat environment for the food and agriculture sector throughout 2026. Organizations should adapt their defenses to address not only the proliferation of smaller, more agile threat actors, but also the layered attack methods and sophisticated technologies that make detection and recovery increasingly challenging. Effective preparedness means anticipating multi-vector attacks that exploit both technical infrastructure and human vulnerabilities.

Built by industry *for industry.*
Defending better by defending together.

FoodandAg-ISAC.org
Membership@FoodandAg-ISAC.org