Food Ag ISAC
An IT ISAC Community

NEW

FARM-TO-TABLE RANSOMWARE REALITIES

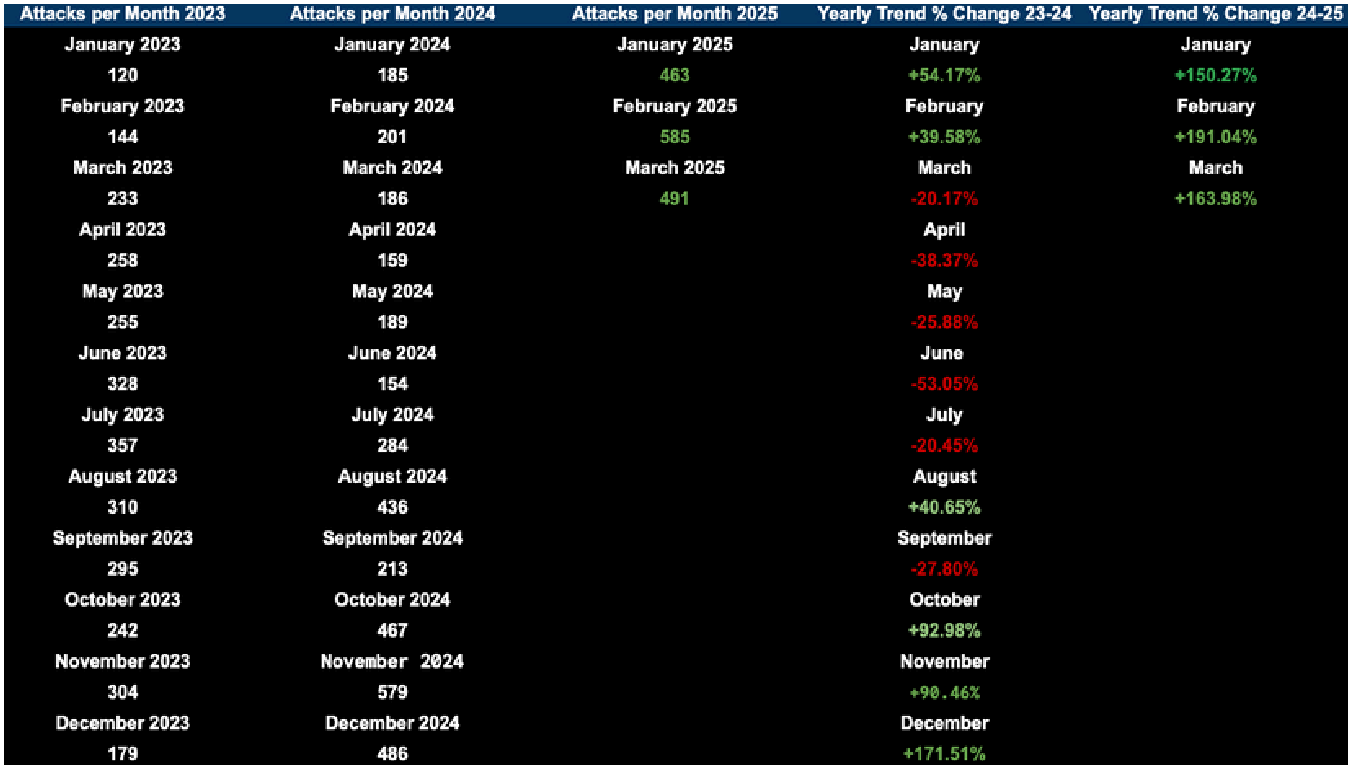
Q1 2025 Analysis
January - March

Q1 2025 Analysis
January - March

The Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC) continues to keep tabs on ransomware attacks against the food and agriculture sector. This tracking enables us to identify prominent ransomware groups who are targeting the sector, analyze their common tactics, techniques, and procedures, and report these findings back to the sector to help organizations bolster their defenses.

Notable Increase in Ransomware Attacks to Begin 2025

The fourth quarter of 2024 saw a notable uptick in ransomware volume across all critical sectors, and the growth in ransomware attacks continued into Q1 2025. This uptick in attack volume is likely attributed to increased activity by several prominent ransomware groups like CL0P, RansomHub, and Akira.



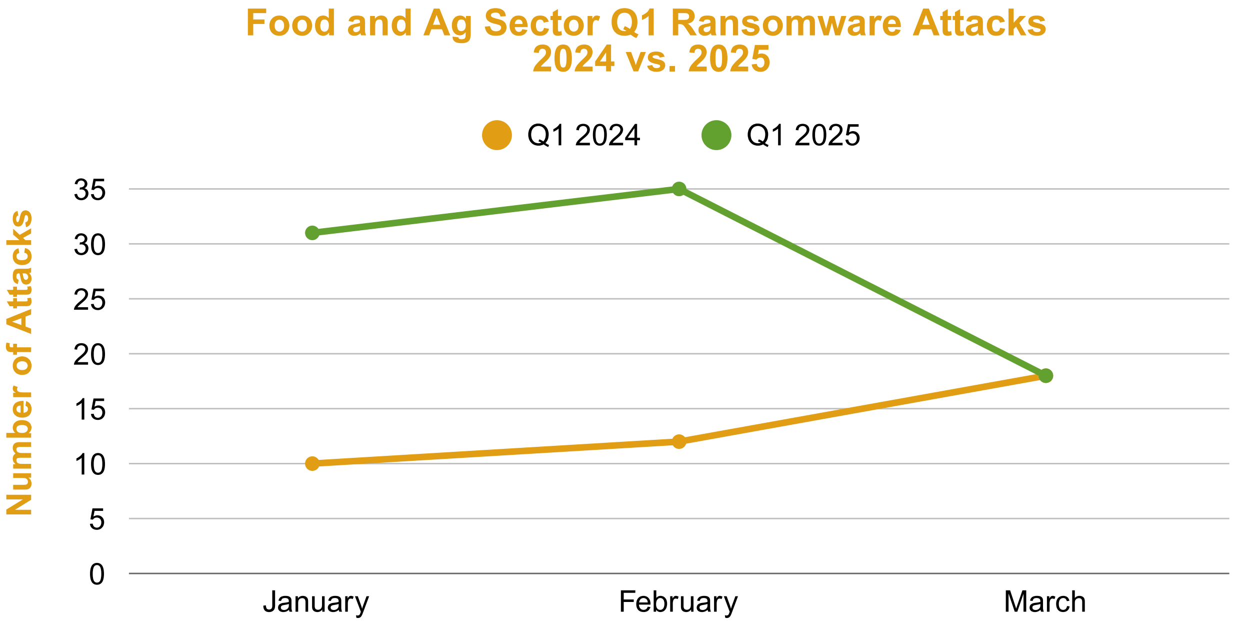
Attacks per Month 2023	Attacks per Month 2024	Attacks per Month 2025	Yearly Trend % Change 23-24	Yearly Trend % Change 24-25
January 2023	January 2024	January 2025	January	January
120	185	463	+54.17%	+150.27%
February 2023	February 2024	February 2025	February	February
144	201	585	+39.58%	+191.04%
March 2023	March 2024	March 2025	March	March
233	186	491	-20.17%	+163.98%
April 2023	April 2024		April	
258	159		-38.37%	
May 2023	May 2024		May	
255	189		-25.88%	
June 2023	June 2024		June	
328	154		-53.05%	
July 2023	July 2024		July	
357	284		-20.45%	
August 2023	August 2024		August	
310	436		+40.65%	
September 2023	September 2024		September	
295	213		-27.80%	
October 2023	October 2024		October	
242	467		+92.98%	
November 2023	November 2024		November	
304	579		+90.46%	
December 2023	December 2024		December	
179	486		+171.51%	

Ransomware Attacks Per Month - Food and Ag-ISAC Ransomware Tracker, 2025

How We Collect Our Data
Note that metrics were obtained via open-source sites, the dark web, member input, and information shared between National Council of ISAC members. Due to outside assistance in monitoring ransomware attacks from partners and third parties, our metrics are likely biased towards the information technology and food and ag sectors.

Q1 2025 Analysis Cont'd

While attacks have risen across all critical sectors, the food and agriculture sector experienced more than three times the number of incidents in January and February 2025 compared to the same period in 2024. In March, however, activity appeared to level off, with 18 reported attacks in the first quarter of both years. Although the monthly number of attacks has stabilized, overall attacks across all sectors remain elevated. Due to the opportunistic nature of ransomware attacks, we expect an overall increase in attacks against the food and agriculture sector in 2025 compared to last year. In the graph below, we highlight the range of attacks in Q1 2025 vs Q1 2024 within the sector.

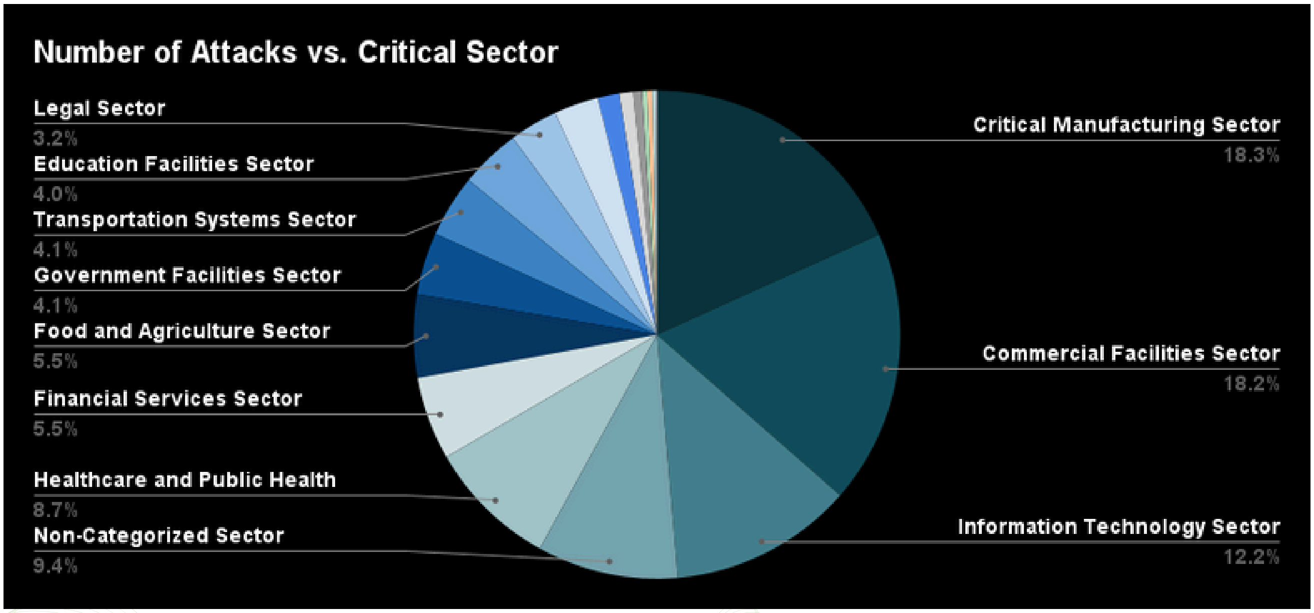


Q1 2025 Analysis Cont'd

How Does the Food and Agriculture Industry Compare to Other Sectors?

Despite the threefold increase in ransomware attacks against the food and agriculture sector, the overall targeting remains fairly consistent, as all sectors have experienced an increase in attacks. The food and agriculture sector was targeted in 5.5% of all ransomware attacks we noted between January and March of 2025, which is consistent with our findings from previous quarters. The critical manufacturing sector continues to be the most heavily targeted sector month-to-month. Ransomware groups likely target organizations in critical manufacturing, as ransomware attacks against manufacturing environments may have a higher (or perceived higher) ransomware payout rate. The manufacturing sector also deals with the challenges of legacy equipment, vulnerabilities in industrial control systems, and patch management, which could make them easier targets for financially motivated cybercriminals.

We noted 84 attacks against the food and agriculture sector in Q1 2025, compared to just 40 in Q1 2024. The food and ag sector ranked 6th out of 13 in relation to all other sectors we tracked. Although we have seen a doubled rate of food and ag sector targeting, it aligns with the trend we have seen across all sectors, with ransomware activity increasing 100 - 200% overall.



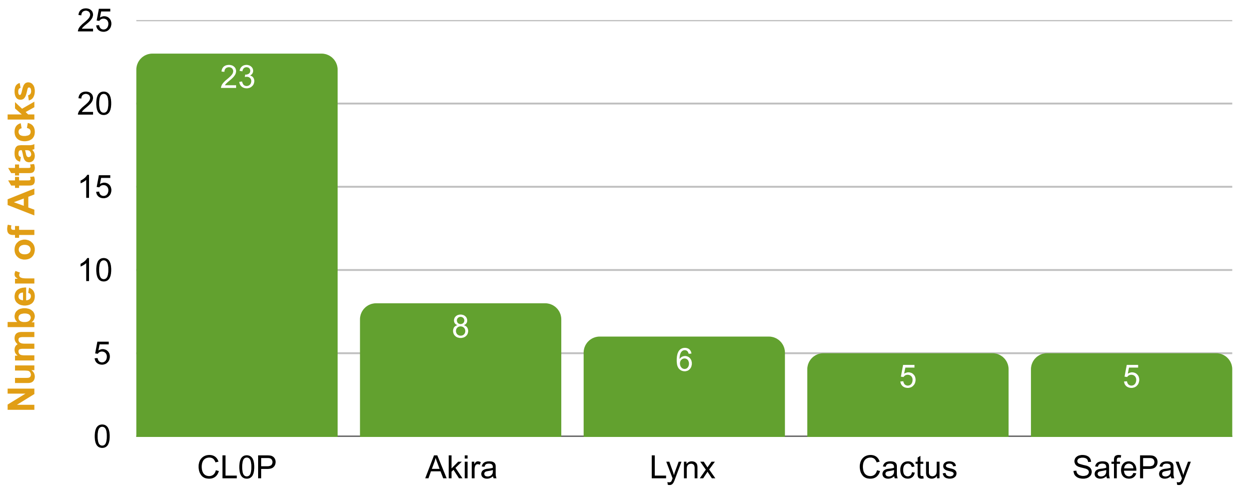
In 2024, the food and agriculture sector was impacted by 5.8% of all 3,494 ransomware attacks we tracked. The Q1 rate of 5.5% shows that while the volume of ransomware attacks may scale up and down, the opportunistic targeting of ransomware attacks has kept the targeting rate relatively the same.

Q1 2025 Analysis Cont'd

Known Actors Hitting the Food and Agriculture Sector

Regardless of where the sector ranks overall in terms of ransomware attacks, ransomware actors remain active in the food and agriculture sector. We tracked 1,537 attacks in Q1 2025; 84 targeted the food and ag sector. Groups like CL0P, who continue to leverage zero-day vulnerabilities in popular file transfer applications to impact hundreds of victims across all critical sectors, are one of the reasons for this ransomware volume surge. However, even if we removed CL0P's proliferation, ransomware attack volume has continued to increase yearly, even as organizations react and adapt to the increasingly sophisticated techniques these groups employ.

Below, we look at the top 5 ransomware groups that impacted the industry in Q1 2025.



Food and Agriculture Sector
Top 5 Ransomware Actors
Q1 2025

Q1 2025 Analysis Cont'd

CL0P

In Q1 2025, we tracked a total of 153 attacks by CL0P across all critical sectors. CL0P is one of the most dangerous ransomware groups due to its targeting of zero-day vulnerabilities. These vulnerabilities are discovered and often exploited before the product vendor is aware. Once a zero-day is discovered, there is usually a period of time between its disclosure and a vendor-issued patch. Threat actors will quickly capitalize on victims during this risky period. Due to poor patch management processes, many organizations remain vulnerable for lengthy periods of time even after a patch is issued.

While the exact methods CL0P uses to discover and exploit zero-day vulnerabilities are not entirely clear, it is believed the group, or the affiliates they work with, have been reverse-engineering popular enterprise products, specifically file transfer applications. According to Kroll, CL0P may test these vulnerabilities for years before carrying out large-scale attacks. Once a vulnerability has been discovered and tested, the group will use mass scanning techniques to locate and exploit victims with exposed instances quickly. It's also possible that CL0P may be purchasing zero-day vulnerabilities and exploits from other cybercriminals on dark web marketplaces.

Below you will find a list of exploited products by the CL0P ransomware group:

- **Accellion FTA**
  - Exploited: December 2020 – March 2021
  - Vulnerabilities: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104
  - Impact: ~100 organizations breached, data theft-only extortion campaign.
- **Fortra GoAnywhere MFT**
  - Exploited: Late January 2023 (zero-day exploit)
  - Vulnerability: CVE-2023-0669
  - Impact: ~130 victims in 10 days, limited to data exfiltration.
- **Progress MOVEit Transfer**
  - Exploited: May 27, 2023 (zero-day)
  - Vulnerability: CVE-2023-34362
  - Impact: 2,100+ victims by December 2023, including U.S. federal agencies.
- **Cleo File Transfer (LexiCom, VLTrader, Harmony)**
  - Exploited: December 2024 – Q1 2025 (zero-day)
  - Vulnerabilities: CVE-2024-50623, CVE-2024-55956
  - Impact: 182+ victims claimed by February 2025.

While there are products that can perform AI/ML-based behavior analysis to prevent zero-day exploitation, these are not a reality for many organizations. Organizations should monitor for current threats and apply patches as soon as they are available. In many cases, zero-day vulnerabilities may still require user interaction, often in the form of phishing and spear phishing. Phishing awareness training and network segmentation can and should be leveraged to thwart potential attacks.

Q1 2025 Analysis Cont'd

Akira

We attributed eight ransomware attacks against the food and agriculture sector to Akira in Q1 2025. In total, Akira was linked to 149 attacks in the first quarter of this year, and the food and agriculture sector accounted for 5.5% of the victims.

Akira is a ransomware-as-a-service (RaaS) that appeared in March of 2023. The group targets organizations across North America, Europe, and Australia in mostly healthcare, engineering, and information technology, but its victimology has also included food and ag companies.

The group's targeting appears quite opportunistic, impacting organizations across many critical sectors and industries, likely due to its use of phishing and compromised credentials for initial access. Akira will frequently target VPN and RDP connections lacking multi-factor authentication, moving laterally to perform network reconnaissance, and use legitimate admin tools like PsExec and WinSCP.

The group exfiltrates data using Rclone and FileZilla and posts the stolen data on their TOR-based data leak site, often issuing ransoms between $400,000 and $2,000,000.

Notably, Akira has targeted VMWare ESXi hypervisors to encrypt entire virtual infrastructures. Throughout 2024, this was the most common method Akira used to breach organizations. They also exploited CVE-2024-40711, a vulnerability in Veeam Backup and Replication, starting in October 2024.

While the group leverages known exploits in popular corporate hardware and software, they also leverage low-sophistication techniques like phishing. Their opportunistic targeting means they are a threat to organizations across all sectors.

Some general mitigations to prevent attacks from Akira include:

- Keeping VPNs and RDP connections patched and enforced with multi-factor authentication.
- Monitoring for unusual data transfers.
- Practicing network segmentation to limit lateral movement.
- Backing up ESXi configurations with immutable storage.

Q1 2025 Analysis Cont’d

Lynx

Lynx, another RaaS, entered the ransomware scene in July of 2024, and shares some similarities with INC ransomware. Notably, the group targets small- and medium-sized businesses (SMBs) globally, with most targets residing in North America, Europe, and Australia. While sectors like retail, manufacturing, and financial services are the most regularly targeted, the group's attacks are widespread and have impacted many critical infrastructure organizations.

The group uses phishing and social engineering, often in the form of fake invoices and urgent alerts, to trick victims into downloading malicious payloads. The group also targets unpatched VPNs, insecure remote desktop protocol (RDP), and has exploited software flaws like CVE-2024-40711 in Veeam Backup. Because the group operates as a RaaS, many different affiliate cyber criminals have different tactics and techniques to breach organizations.

Like many other RaaS operations, the group not only encrypts systems but steals data, which it leaks on its TOR-based ransomware leak website if ransom demands are not met.

Lynx has been responsible for several disruptive attacks targeting US critical infrastructure. Their focus on SMBs highlights Lynx as a continued threat.

Here are some ways you can prevent Lynx:

- Prioritizing updates for VPNs, RDP, and backup software.
- Mandating phishing awareness training.
- Enforcing MFA and least-privilege principles.
- Implementing immutable air-gapped backups (Lynx may target cloud backups).
- Monitoring for anomalous traffic, like data transfer from tools like RClone.

Q1 2025 Analysis Cont'd

Cactus

A double-extortion RaaS operation, Cactus, was first discovered in March of 2023. This group targets enterprises across the globe, often exploiting VPN vulnerabilities for initial access. While some ransomware operations have started simplifying stealing sensitive data for ransom, Cactus does continue to encrypt systems on top of data theft and extortion.

Notable to Cactus is their ability to avoid detection by self-encrypting their payloads, terminating antivirus processes, and deleting shadow copies. The group often leverages RClone for data exfiltration, uploading sensitive documents to their data leak website.

The group typically uses VPN vulnerabilities for initial access, but has also used Qlik Sense flaws (a data analytics platform) as alternate entry points. Additionally, Cactus has used CVE-2023-38035 in Fortinent VPNs, and CVE-2024-40711 in Veeam to breach victim environments.

To maintain persistence, Cactus will create SSH backdoors via scheduled tasks. The group uses tools like SoftPerfect Network Scanner and PSnmap for network reconnaissance, and spreads via RDP and remote monitoring and management (RMM) tools like AnyDesk or Splashtop.

To limit your exposure to Cactus, we encourage the following:

- Patch VPNs/public-facing apps (prioritize CVEs like CVE-2023-38035).
- Monitor for Rclone/PSnmap activity and unusual SSH connections.
- Enforce MFA and segment networks to limit lateral movement.

Q1 2025 Analysis Cont'd

SafePay

SafePay first appeared in October of 2024 as a RaaS operation. The group targets organizations globally in sectors like healthcare, financial services, and manufacturing. The ransomware shows strong ties to LockBit 3.0, which was leaked online, suggesting it was derived from the leaked source code.

For initial access, SafePay will leverage phishing to steal credentials or brute force unsecured RDP/VPN connections. To avoid detection, SafePay will disable Windows Defender via living off the land binaries (LOLBins) and will use tools like ShareFinder.ps1 to scan networks for shared drives.

SafePay touts its rapid encryption of victim networks, claiming to achieve encryption within 24 hours of compromise. We noted 54 attacks by SafePay in Q1 2025, with nearly 9% being attributed to the food and agriculture sector.

SafePay has been a nuisance due to their continued targeting of critical infrastructure.. Known for its speed, ties to LockBit, and focus on North America, SafePay will continue to be an actor to watch in 2025.

General mitigation recommendations include:

- Patching RDP/VPNs and enforcing MFA.
- Monitoring for suspicious PowerShell/WinCMD activity.
- Ensuring Air-gapped backups to prevent encryption.

Takeaways

Ransomware is and will continue to be an ongoing threat to all critical sectors, as it remains profitable and easy to deploy. From the time we produced our first ransomware reports in 2023, the attack volume has grown in the food and ag sector - this trend can be attributed to the sector's growing dependence on technology and need for just-in-time operations.

While every sector faces distinct challenges in responding to ransomware, the food and agriculture industry contends with its unique issues. The tightly timed supply chains and product delivery may make organizations in this sector especially appealing to ransomware operators seeking quick leverage. Beyond financial impact, the potential implications for health and human safety can further intensify the pressure on companies during an incident.

While the sector continues to experience ransomware attacks, much of the targeting still appears to be opportunistic. Many of the groups targeting the sector have targeted other sectors at an equal or greater rate, and there are no specific patterns seen in the victimology.

Food Ag ISAC

An IT ISAC Community

MEMBERSHIP@FOODANDAG-ISAC.ORG

FOODANDAG-ISAC.ORG