Food Ag ISAC
An IT ISAC Community

NEW

FARM-TO-TABLE RANSOMWARE REALITIES

Q2 2025 Analysis
April - June

Q2 2025 Analysis
April - June

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

Continued Increase in Ransomware Attacks Across All Sectors into Q2

The ISAC noted a significant uptick in ransomware volume starting in the fourth quarter of 2024 across all sectors. This increase continued into the first quarter of 2025. Although the volume has decreased slightly in Q2, it remains significantly higher than in the previous year. Initially, we suspected the increase to be related to CL0P's exploitation of a significant vulnerability in Cleo Harmony (CVE-2024-50623 and CVE-2024-55956), but ransomware volume has continued to be elevated even after CL0P-related attacks have ceased. Several ransomware groups, including Qilin, Akira, and SafePay, have contributed to the steady increase of ransomware attacks in Q2 of 2025.

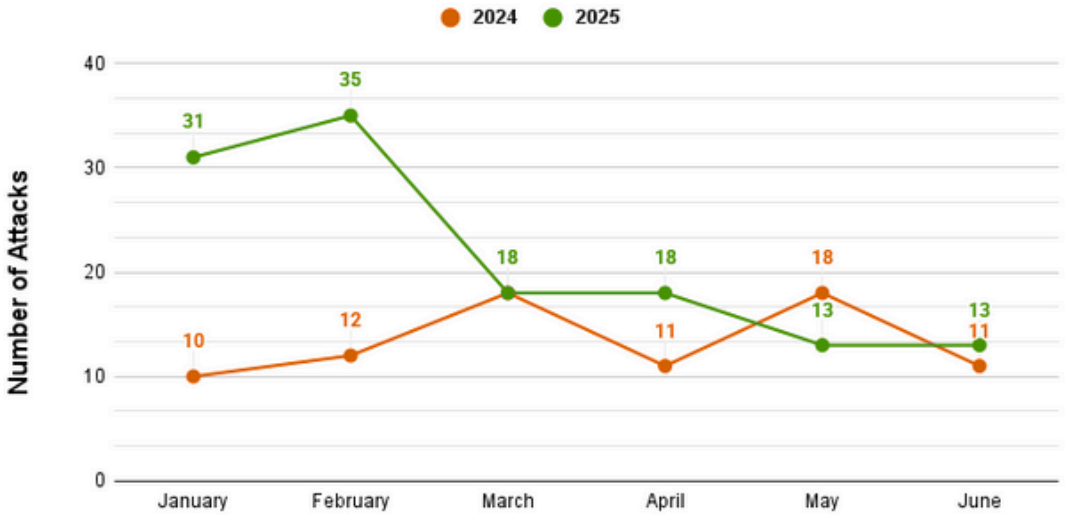
Attacks per Month 2023	Attacks per Month 2024	Attacks per Month 2025	Yearly Trend % Change 23-24	Yearly Trend % Change 24-25
January 2023	January 2024	January 2025	January	January
120	185	463	+54.17%	+150.27%
February 2023	February 2024	February 2025	February	February
144	201	585	+39.58%	+191.04%
March 2023	March 2024	March 2025	March	March
233	186	489	-20.17%	+162.90%
April 2023	April 2024	April 2025	April	April
258	159	446	-38.37%	+180.50%
May 2023	May 2024	May 2025	May	May
255	189	463	-25.88%	+144.97%
June 2023	June 2024	June 2025	June	June
328	154	379	-53.05%	+146.10%
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

Q2 2025 Analysis
April - June

Noted Decrease in Ransomware Attacks Against the Food and Agriculture Sector

In Q1 2025, we noted an increase in attacks against the food and agriculture sector, with attacks in January and February up almost 300% from the previous year. This number has fortunately stabilized in Q2, with a similar number of attacks to what we noted in 2024. Although the attack volume decreased in Q2, we still observed 44 attacks against the sector, underscoring the fact that ransomware remains a top threat.



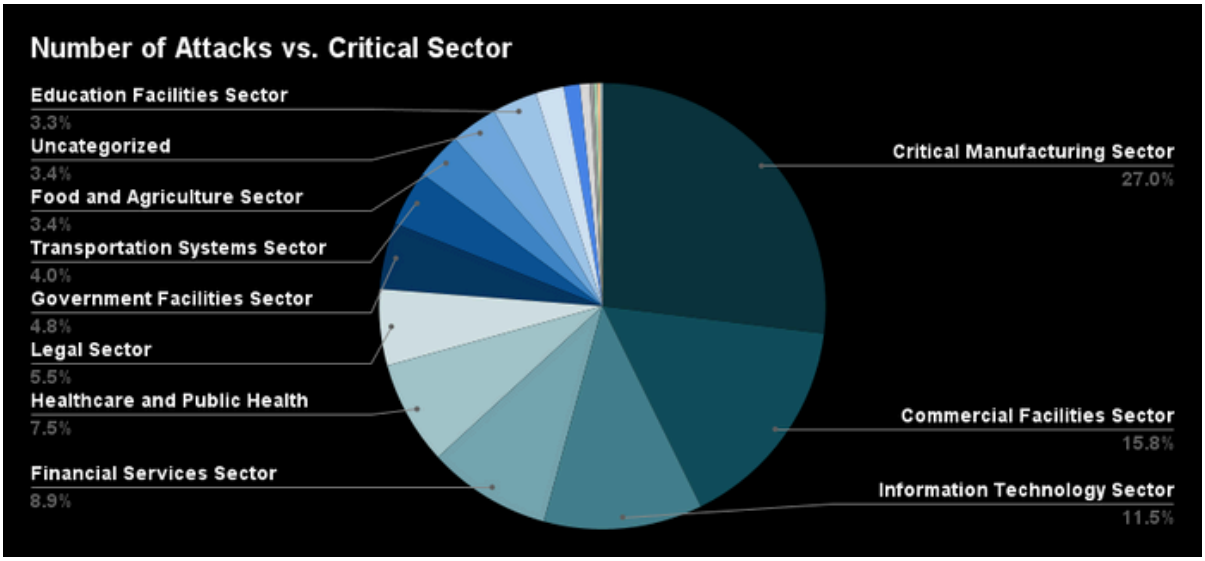
How Does the Food and Agriculture Industry Compare to Other Sectors?

Ransomware attack volume across all sectors has increased in 2025, but Q2 shows signs of stabilization. We tracked 1,288 ransomware attacks in Q2 of 2025, and only 44 of those were against the food and agriculture sector, representing 3.4% of all attacks. In comparison, in Q1, 84 attacks observed against the sector represented 5.5% – however, the sheer number of attacks across all sectors was higher..

Month by month, the critical manufacturing sector remains the most targeted sector, accounting for over a quarter of all tracked ransomware attacks. Ransomware groups are likely to target organizations in critical manufacturing, as ransomware attacks against manufacturing environments may have a higher (or perceived higher) ransom payout rate. The manufacturing sector also faces challenges such as legacy equipment, vulnerabilities in industrial control systems, and patch management, which can make it an easier target for financially motivated cybercriminals.

While the percentage of ransomware attacks decreased in Q2, the opportunistic nature of these attacks could cause this trend to quickly change in future quarters. The sector should remain vigilant against the threat of ransomware and continue to monitor and understand major ransomware actors, tactics, and defenses.

Q2 2025 Analysis
April - June

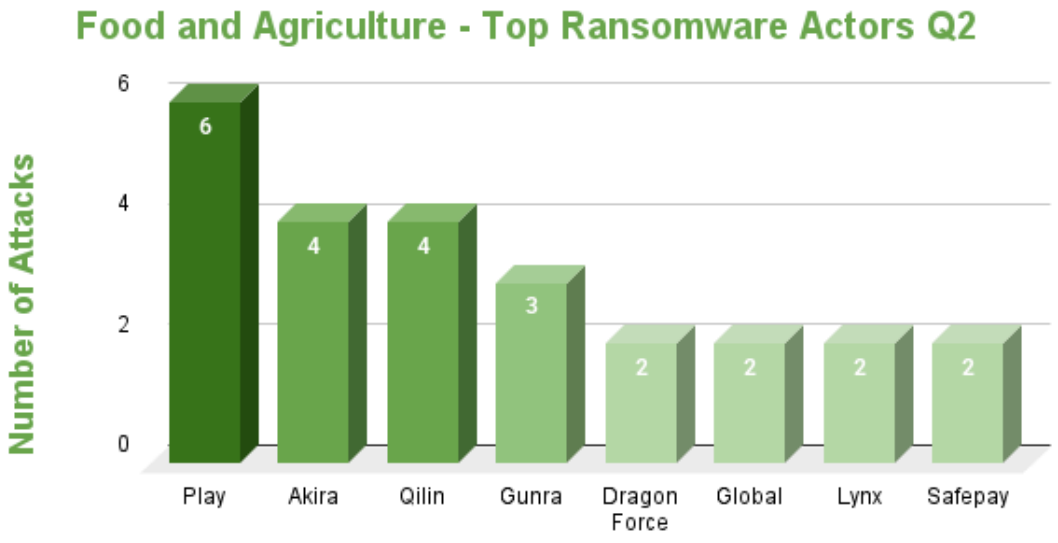


In 2024, the food and agriculture sector was impacted by 5.8% of all 3,494 ransomware attacks we tracked. The Q2 rate of 3.4% is down from our average; however, ransomware attacks can scale up and down, and the opportunistic targeting of these attacks has kept the targeting rate relatively constant.

Known Actors Hitting the Food and Agriculture Sector

We tracked 26 different ransomware groups targeting the food and agriculture sector in Q2 2025, though only a few were responsible for multiple attacks. Most of the groups targeting the food and agriculture sector are also among the top groups for other sectors, with the exception of Play, which has a disproportionately high rate of observed attacks in the sector (7.5% of all attacks). Absent from this list is CL0P, which has gone relatively silent since its aggressive and impactful exploitation of Cleo Harmony towards the end of Q4 2025 into early 2025. CL0P's widespread attacks in early 2025 were responsible for a portion of the significant uptick in attacks against the sector in Q1.

Below, we look at the top ransomware groups that impacted the industry in Q2 2025.



Q2 2025 Top Ransomware Groups
April - June

Play

The Play ransomware group has been responsible for 43 attacks against the food and agriculture sector since we began tracking them. At 7.5% of attacks, their targeting of the sector is fairly significant. We noted six attacks against the sector that originated from them in Q2 of 2025.

Play appeared in 2022 and has been active ever since. The ISAC has identified nearly 600 attacks attributed to the group. Play is known to target public-facing and vulnerable systems, including FortiOS, Microsoft Exchange, and various RMM tools. They may also leverage legitimate Virtual Private Network (VPN) and Remote Desktop Protocol (RDP) credentials, which may be purchased from initial access brokers.

The group uses living-off-the-land (LOTL) tactics to remain hidden on victim networks, stealthily exfiltrating data before allowing their custom ransomware strain to encrypt systems. The group uses TOR for communication with victims, including negotiation and threats to publish stolen data on a data leak website.

The group is known to target U.S. critical infrastructure entities, and CISA has released a #StopRansomware report on the group.

Akira

We attributed four ransomware attacks against the food and agriculture sector to Akira in Q2 2025, down from eight attacks in the previous quarter. In total, Akira was linked to 116 attacks in the second quarter of this year, and the food and agriculture sector accounted for 3.4% of the victims. Akira heavily targeted the critical manufacturing sector, which accounted for over 40% of its attacks.

Akira is a ransomware-as-a-service (RaaS) that emerged in March 2023. The group primarily targets organizations across North America, Europe, and Australia, with a focus on healthcare, engineering, and information technology sectors; its victimology has also included food and agriculture 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 utilize legitimate administrative tools, such as PsExec and WinSCP.

The group exfiltrates data using Rclone and FileZilla, then posts the stolen data on their TOR-based data leak site, often issuing ransoms ranging from $400,000 to $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 employ low-sophistication techniques, such as phishing. Their opportunistic targeting makes them a threat to organizations across all sectors.

Q2 2025 Top Ransomware Groups
April - June

Qilin

Across all sectors in Q2, we tracked 166 attacks by Qilin. Four of these attacks targeted entities in the food and agriculture sector, which accounted for only 2.4% of their total targets. While Qilin directed roughly 24% of its attacks toward the critical manufacturing sector, its activity reflects a broad and opportunistic approach. The food and agriculture sector is not their typical target, but the sheer volume and indiscriminate nature of their campaigns make it likely that food and agriculture companies could become victims.

Originally referred to as Agenda, the group emerged in 2022 as a RaaS. Qilin is a significant ransomware actor, known for targeting a large number of victims across various industries.

Their ransomware strain is custom-built and can impact Windows and Linux systems. The group employs a double extortion tactic, stealing data and encrypting systems. Affiliates of Qilin will typically leverage targeted spearphishing attacks, exploitation of public-facing applications, and may purchase compromised credentials for initial access.

We have tracked over 400 attacks by Qilin since their inception, making them a prominent and impactful ransomware actor.

Gunra

We only tracked nine attacks by Gunra in Q2 of 2025, but three of those were against the food and agriculture sector. Gunra is a relatively new ransomware strain, believed to have emerged in April 2025. The group carries out double extortion attacks, stealing data, encrypting systems, and deleting backups. They use TOR for negotiations with victims.

For initial access, the group leverages phishing emails to steal credentials and likely purchases additional credentials from initial access brokers. Like many ransomware groups, Gunra will exploit unpatched and vulnerable public-facing applications. In some cases, they may attempt to brute-force RDP for initial access.

Gunra is written in C/C++ and was likely developed from the leaked Conti ransomware strain. Although the group is relatively new, it appears to be aggressively working to impact organizations. The large percentage of food companies in their relatively small targeting volume makes them a group to monitor for the sector.

Q2 2025 Top Ransomware Groups
April - June

Dragon Force

The ISAC has tracked 82 attacks by Dragon Force since its emergence, and 29 attacks specifically targeting the food and agriculture sector. In Q2, two food and agriculture companies fell victim to the group. While not a staggering number of attacks, it represented almost 8% of the group's observed attacks.

While the group's origins go back to 2023, it wasn't until early 2024 that they became an official and active RaaS operation offering services and a data leak website. It is likely that Dragon Force was built from the leaked LockBit 3.0 source code, as it shares many code similarities. In mid-2024, they adopted and modified the Conti v3 source code, enhancing their capabilities for Windows, Linux, ESXi, and NAS targets.

The group carries out double extortion attacks, stealing and encrypting data before issuing a ransom to victims. For initial access, the group will leverage spearphishing, which also includes vishing and smishing. They may also mimic legitimate SSO portals to steal credentials. Additionally, they will exploit known vulnerabilities in public-facing applications, purchase stolen credentials, and attempt to brute-force VPN and RDP connections.

More recently, the group has appeared to have teamed up with Scattered Spider, a prominent cybercriminal gang, which is using Dragon Force as an encryptor after carrying out high-profile breaches. DragonForce has been particularly active in early to mid-2025, claiming responsibility for high-profile breaches against major UK retailers, including Marks & Spencer (M&S), the Co-op Group, and Harrods.

Global

Global is a relatively new strain of ransomware. In Q2, we tracked 18 attacks by the group, with two of those in the food and agriculture sector. The group seems to show a preference for the critical manufacturing and healthcare sectors.

Global appears to have emerged in Q2 of this year and has already listed several larger victims on the data leak website – including a major private healthcare institution in Australia and a leading UK-based automotive body shop.

The group has shown a preference for critical infrastructure targets and should remain monitored by food and agriculture companies.

Q2 2025 Top Ransomware Groups
April - June

Lynx

Lynx, another RaaS, entered the ransomware scene in July 2024, and shares some similarities with INC ransomware. Notably, the group impacts small- and medium-sized businesses (SMBs) globally, with most victims 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 employs phishing and social engineering tactics, often in the form of fake invoices and urgent alerts, to deceive victims into downloading malicious payloads. The group also exploits unpatched VPNs, insecure RDP, and software flaws like CVE-2024-40711 in Veeam Backup. Because the group operates as a RaaS, various affiliate cybercriminals employ 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.

SafePay

SafePay first appeared in October 2024 as a RaaS operation. The group targets organizations worldwide in sectors such as 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 utilize phishing to steal credentials or attempt brute force attacks on unsecured RDP/VPN connections. To avoid detection, SafePay will disable Windows Defender using living-off-the-land binaries (LOLBins) and utilize 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 its continued targeting of critical infrastructure. Known for its speed, ties to LockBit, and focus on North America, SafePay will continue to be a key player to watch in 2025.

Q2 2025 Ransomware Actor Trends

April - June

We saw the emergence of several new players in Q2. Groups like LockBit, RansomHub, and CL0P, who were active in previous quarters, have been replaced by some new groups, namely Qilin, Dragon Force, Akira, Play, SafePay, DevMan, BERT, and Gunra.

As law enforcement continues to combat prominent ransomware actors, the affiliates working with these RaaS operations regroup with new strains, fragmenting the ecosystem. This constant shifting and restructuring make it difficult to monitor for specific strains and tactics.

While we saw a brief trend of ransomware groups foregoing the encryption of systems to instead only steal data, many groups are again opting to encrypt systems while wiping backups and cloud storage options. This disruption of service proves to be a major motivation for victims to pay the ransom demands, especially against critical infrastructure entities.

Additional forms of extortion remain common. Distributed Denial of Service (DDoS) can be used to further pressure victims into paying. Public harassment has also been reported, directly contacting victims' employees, customers, and partners via phone, email, and text to pressure them. Artificial intelligence (AI) and machine learning (ML) continue to be utilized to enhance the quality of phishing emails, automate voice phishing (vishing), and support reconnaissance and vulnerability scanning.

Scattered Spider has been collaborating with Dragon Force to conduct high-profile attacks against organizations across multiple industries. The group has been employing help desk impersonation attacks, deceiving IT help desks into granting them access to accounts or resetting passwords/MFA settings for important employees.

Lastly, ransomware groups continue to exploit recent vulnerabilities, with proof-of-concept code available, quickly capitalizing on the vulnerable window where victims are discovering and patching against emerging vulnerabilities.

Q2 2025 Takeaways

April - June

The ISAC continues to monitor ransomware attacks in an effort to understand active groups, their sector targeting, tactics, and general ransomware landscape trends. Ransomware is a threat to all critical sectors, impacting organizations of all shapes and sizes. The food and agriculture sector continues to integrate technology into farms, which requires organizations to manage, update, and protect an ever-growing list of systems and products. The sector's growing dependence on this technology and its need for just-in-time operations make it an ideal target for ransomware operators. While ransomware represents an ideal target for ransomware attacks, much of our data points towards more opportunistic attacks. 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.

While global law enforcement has carried out operations against major ransomware players, we continue to note a continued increase in ransomware attacks every year. New players have entered the ransomware landscape, leading to an increase in attacks, and several prominent cybercriminal collectives (Scattered Spider & FIN11) have joined, or continue to leverage ransomware attacks due to its profitability and obscurity via the ransomware-as-a-service model. Additionally, several nation state actors (Lazarus, ChamelGang, APT41) have added ransomware to their arsenal as a means to obscure their true intent of cyber espionage.

While ransomware attacks against the food and agriculture sector have stabilized in Q2 of 2025, the sector continues to see a significant number of attacks, including some against major supply chain entities like United Natural Foods, Inc. (UNFI), Coca-Cola, Marks & Spencer and Co-op Group. Sector entities should continue to monitor prominent ransomware groups and stay up to date on their latest tactics, techniques, procedures, and extortion tactics.

Food Ag ISAC

An IT ISAC Community

MEMBERSHIP@FOODANDAG-ISAC.ORG

FOODANDAG-ISAC.ORG

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 agriculture sectors.