Food Ag-ISAC

STATE OF THE THREAT

Food and Agriculture Sector Cyber Trends

AUGUST 2026

OVERVIEW

Food and agriculture organizations spent the first half of 2026 fending off a threat landscape that is expanding on nearly every front at once. The Food and Ag-ISAC, in partnership with the IT-ISAC, tracks over 330 adversaries through ongoing threat intelligence work, member collaboration, and partner reporting across the security community. Based on this, six trends have emerged in 2026:

AI: MORE CVEs, LESS RUNWAY
Defenders and attackers have both integrated AI into daily operations, from AI-assisted “vibe-coding” to increasingly autonomous farm and processing equipment. The result is a surge in disclosed vulnerabilities paired with a shrinking window to act on them, which makes prioritization, not coverage, the central patching challenge.

RANSOMWARE: VOLUME KEEPS CLIMBING
Ransomware attacks against the food and agriculture sector surged 29% in 2025 to 295 recorded incidents. Through July 2026, the sector has already recorded 227 incidents, a 62% increase over the same period in 2025.

NATION-STATES: PLAYING THE LONG GAME
These actors continue to broaden their attacks beyond traditional espionage, planting themselves inside critical infrastructure and slipping onto companies' payrolls.

HACKTIVISTS: BLURRING THE LINE
Hacktivist groups are taking sides in geopolitical conflicts and shifting tactics from defacement and denial-of-service campaigns to destructive attacks on operational environments.

TYPOSQUATTING: PROFITING FROM A TYPO
Criminal groups are registering lookalike domains that impersonate food and agriculture companies and their suppliers, fueling business email compromise (BEC) schemes that redirect payments and steal credentials across the farm-to-table supply chain.

CLICKFIX: EVOLVING SOCIAL ENGINEERING
This attack is widely used across threat actor groups. This attack tricks users into pasting and running malicious commands under the guise of fixing a fake error message, and has become one of the fastest-growing ways for attackers to gain an initial foothold.

Taken together, these trends underscore a rapidly evolving landscape that requires constant vigilance and near-real-time adjustments by network defenders.

AI: MORE CVEs, LESS RUNWAY

No trend has moved faster in 2026 than AI adoption on both sides of the fight. What used to be a multi-year technology adoption curve has compressed into months. AI has become a genuine advantage for defenders, but attackers are benefiting from the same acceleration.

For food and agriculture security teams stretched thin, AI is helping close the gap by triaging alerts, correlating signals, and flagging anomalies that rule-based tools would miss, like unusual data downloads or a service account accessing new systems. The gap it is closing is real, as AI-assisted triage helps security teams keep pace with the alert volume a modern, connected operation generates.

That connected footprint is also expanding fast. Farm and processing equipment is growing more autonomous, from GPS-guided tractors and robotic harvesters to automated feed mills and self-adjusting cold storage systems. The attack surface is growing faster than most teams can inventory. Every networked grain silo sensor, automated feeder, and cold-chain thermometer is a potential entry point for lateral movement, part of what can be referenced as a "shadow operational technology (OT)" problem. These operational devices are added for efficiency and often go unseen by traditional IT asset management. AI-assisted monitoring helps surface that shadow inventory and flag when one of those devices starts behaving abnormally, something a team relying on manual log review would likely miss until too late.

In addition, AI-assisted vulnerability discoveries are driving a surge in disclosed vulnerabilities. For example, CVE disclosures are on pace to hit 66,000 in 2026, running 46.3% ahead of projections released by FIRST. In 2025, of the roughly 48,000 CVEs disclosed, only about 1% were actually exploited. Whether that gap between disclosure and exploitation will hold in 2026 and beyond remains to be seen. However, for a sector where OT, including the programmable logic controllers (PLCs) that run processing lines, irrigation, and grain handling equipment, is increasingly internet-connected, this trend is especially consequential. Compounding this, the same tooling that surfaces vulnerabilities is compressing the time to weaponize them. Proof-of-concept exploit code that once took days to develop can now be generated in hours. Exploitation remains narrow, but arrives fast, and that combination of volume and velocity is what makes triage, not coverage, the defining patch management challenge. Network defenders cannot treat every new CVE as equally urgent, and exposed OT and ICS components deserve heightened scrutiny.

The "patch everything, patch now" approach that often works for other organizations, such as a cloud-native IT shop, is not realistic in the food and agriculture sector. A processing line cannot be taken offline mid-harvest to apply an update, and many of the PLCs and sensors running that line may be years old, possibly running firmware that may not have a patch available. Most security teams lack the bandwidth to chase every CVE that crosses their feeds. Instead, they need to know which vulnerabilities in their environment are actually likely to be exploited. They can then prioritize those and wait until the next scheduled maintenance window for lower-risk vulnerabilities.

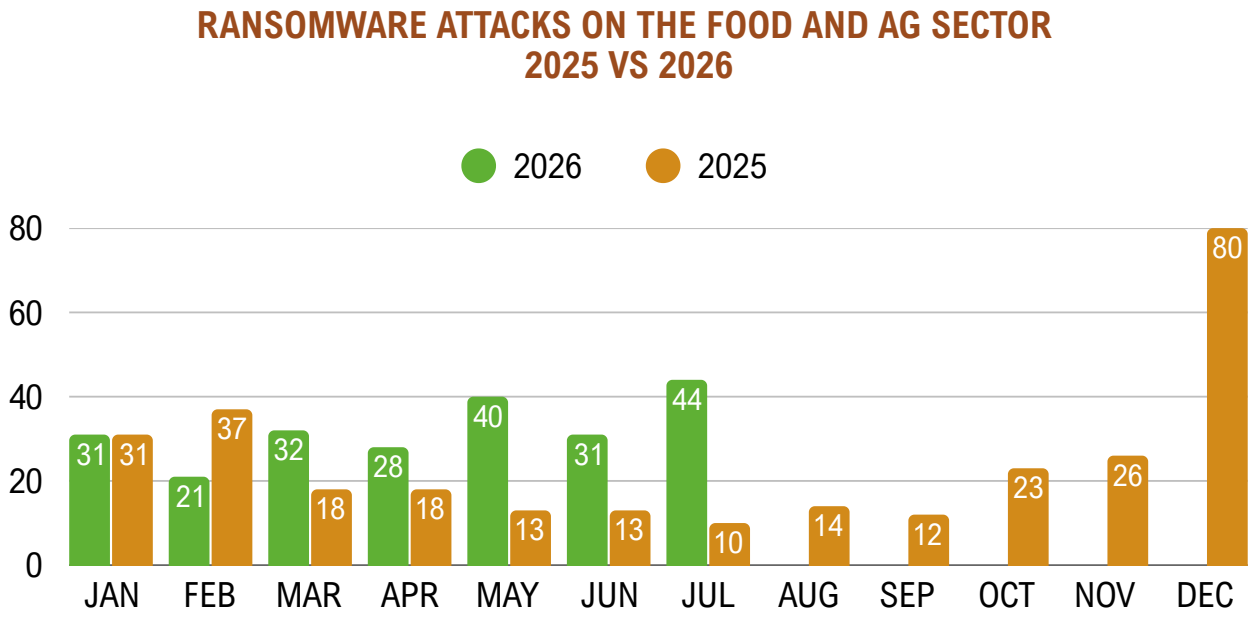
Fortunately, the following two free resources can help companies make risk-informed patch management decisions:

- **CISA BOD 26-04**
  CISA's Binding Operational Directive 26-04 provides a structured framework for prioritizing security updates based on real-world risk factors including public exposure, presence on the Known Exploited Vulnerabilities (KEV) catalog, and technical impact.

- **Exploit Prediction Scoring System (EPSS)**
  Developed by FIRST, EPSS uses machine learning to identify patterns between vulnerability characteristics and observed exploitation activity, offering a substantially better predictor of real-world exploitation than CVSS thresholds alone.

RANSOMWARE: VOLUME KEEPS CLIMBING

Ransomware remains the most consistent and costly threat facing the food and agriculture sector. Unfortunately, 2026 is on pace to be one of the highest-volume ransomware years on record. Through July, the Food and Ag-ISAC, in partnership with the IT-ISAC, tracked 4,272 successful ransomware attacks across 108 unique threat groups, up 22.7% over the same period in 2025 (4,381 attacks) and 219.5% over the same period in 2024 (1,337 attacks).



Through July, the food and agriculture sector accounted for 227 ransomware incidents, a 62% increase from the 140 attacks recorded during the same period in 2025. The Qilin ransomware group was the most active toward the sector with 47 listed attacks, followed by The Gentlemen (31), and Akira (14). These incidents represented roughly 5% of all attacks tracked into July, ranking food and agriculture as the eighth most-targeted sector.

While some attacks are targeting food and agriculture companies specifically, overall ransomware attacks remain largely opportunistic. Most campaigns scan for exposed systems, acquire access through brokers, and rely on phishing and social engineering to compromise the first vulnerable organization that surfaces. Food and agriculture entities are swept up in that high-volume, indiscriminate activity as much as they are deliberately singled out.

NATION-STATES: PLAYING THE LONG GAME

Nation-state activity has intensified in 2026 as actors expand their playbook well beyond traditional espionage. Their cyber activities are driven by strategic intent and in support of national objectives, including intelligence collection, military preparation, revenue generation, and the ability to disrupt critical infrastructure during a future conflict. This year's activity spans everything from increased, quiet pre-positioning inside critical infrastructure to brazen workforce fraud schemes, and nation-state threats show no signs of slowing down.

For food and agriculture organizations, that distinction matters because nation-state actors are often playing a longer game than financially motivated criminals. These actors seek access, intelligence, or leverage that doesn't always need to be used immediately. In the Food and Ag-ISAC's most recent threat report, nation-state actors represented the second-largest category of adversaries targeting the sector, behind ransomware groups.

China's activity is a clear example of strategic cyber positioning. They are not hiding what they are after, as cyberspace dominance is a stated pillar of their national strategy. As part of this strategy, Chinese operators are pre-positioning inside U.S. critical infrastructure, laying the groundwork for disruption if a conflict calls for it. For food and agriculture, the concern extends beyond operational systems disruption. Chinese actors have also demonstrated sustained interest in intellectual property, research, and technologies associated with seeds, agricultural chemicals, biotechnology, and food production. This makes the sector valuable both as critical infrastructure and as a source of economic and technological intelligence.

Russia combines traditional state-sponsored activity with a much broader range of actors whose relationship with the government can be difficult to define. Russian state-sponsored operators continue targeting critical infrastructure and exploiting vulnerable networking equipment to establish persistent access and collect intelligence. A joint cybersecurity advisory in July 2026 highlighted activity tied to the Russian Federal Security Service's (FSB) Center 16, which has targeted vulnerable network infrastructure across multiple critical infrastructure sectors. The activity has been associated with threat groups tracked under names including Berserk Bear, Energetic Bear, Crouching Yeti, and Dragonfly.

Iran tends to blur the line between state operations and hacktivism, but it has shown a willingness to target food security directly. The FBI, EPA, and CISA confirmed attackers were exploiting internet-exposed programmable logic controllers (PLCs), the same class of equipment that runs processing lines, cold storage, and grain handling systems across food and agriculture. Formal attribution is still pending, but federal officials have pointed to tradecraft consistent with prior Iranian operations.

North Korea, the Democratic People's Republic of Korea (DPRK), meanwhile, continues dispatching thousands of skilled IT workers to pose as freelancers or full-time remote employees, including at food and agriculture companies building out their IT and data science functions. They use stolen identities, laptop farms to fake a U.S. location, and crypto payment chains to launder their wages back to the regime. What started as a salary-collection scheme has evolved into something riskier: data theft, source code exfiltration, extortion, and insider access sold to other threat actors.

Learn more about DPRK workers and signs to watch for here.

HACKTIVISTS: BLURRING THE LINE

Hacktivism against food and agriculture is not always as clear-cut as it looks on the surface, but it is increasingly significant during periods of geopolitical conflict. Unlike traditional nation-state actors, hacktivists are typically politically or ideologically motivated and operate without confirmed direct state control. According to the most recent Food and Ag-ISAC Cyber Threat Report, hacktivists account for 9.7% of the adversary types tracked across more than 330 actors. Their goal is often visibility through disruption, whether by amplifying a political message, embarrassing a target, or simply creating chaos.

Historically, hacktivist activity has relied on relatively accessible tactics such as distributed denial-of-service (DDoS) attacks, website defacements, data leaks, credential attacks, and exaggerated claims of compromise. In 2026, however, some hacktivist groups are reaching further into operational environments, making the consequences potentially more significant even when the underlying techniques remain comparatively simple. This includes internet-accessible systems such as human-machine interfaces (HMIs), SCADA environments, and automatic tank gauges (ATGs). CISA and its partners have urged organizations to harden internet-connected ATGs, which monitor fuel and other liquid storage tanks and have been targeted by cyber actors exploiting exposed or poorly secured devices.

Dark Engine is one example of a notorious hacktivist group often characterized as a state-aligned collective with geopolitical ties to Eastern Europe. They are known for targeting HMIs that control automated machinery. If this type of attack succeeds, it could halt production lines, disrupt irrigation systems, or interfere with temperature-controlled storage.

Recent geopolitical events have shown how quickly hacktivist activity can surge. Following Operation Epic Fury, Rescana tracked 149 distributed DDoS claims against 110 organizations across 16 countries. The activity showed a heavy concentration against supervisory control and data acquisition (SCADA) systems, the software that runs industrial and agricultural equipment, and echoes CISA's 2025 warning that pro-Russia hacktivists are actively targeting food and agriculture's internet-facing OT alongside water and energy.

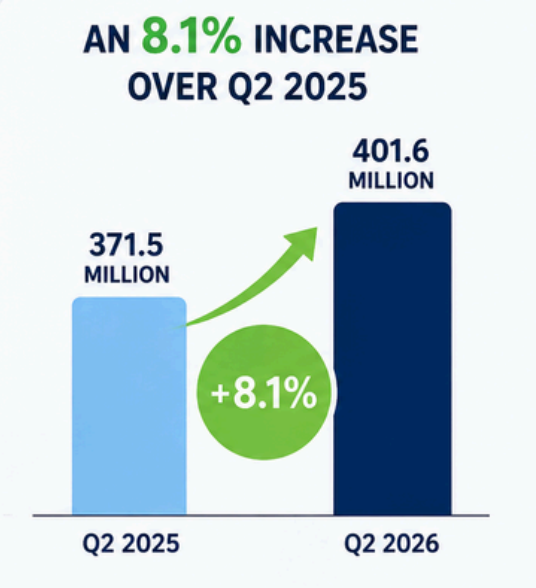
The distinction between hacktivism and nation-state activity is increasingly blurred. Pro-Russia groups such as Cyber Army of Russia Reborn, NoName057(16), Z-Pentest, and Sector16 present themselves as hacktivists while advancing Russian geopolitical interests, and some may receive indirect government support. Iran has taken this further, with personas such as CyberAv3ngers and Handala using hacktivist branding despite later links to the IRGC or Ministry of Intelligence and Security. For food and agriculture organizations, this means “hacktivist” should not be assumed to mean low-impact or independent, particularly as politically motivated actors increasingly target exposed OT.

TYPOSQUATTING: PROFITING FROM A TYPO

Typosquatting, which means registering domains that are intentional misspellings or close variations of a legitimate company's name, has become one of the most common enablers of business email compromise (BEC) and payment fraud across the food and agriculture sector. Attackers use these lookalike domains to impersonate a supplier, a customer, or an executive, timing fraudulent invoices or payment redirection requests to look indistinguishable from routine business correspondence.

The technique is not limited to email or to true misspellings. Lookalike domains are also used to host cloned vendor portals and payment pages, and increasingly pair with AI-generated deepfake audio or video to impersonate an executive's voice on a call. The Food and Ag-ISAC has been tracking these fraudulent domains with the help of members and partners and has found that the majority target the food processing and manufacturing vertical within the sector. This is the point in the supply chain where invoicing and payment volume between suppliers and buyers is highest.

Just like the other trends outlined, typosquatting is only picking up speed. The Domain Name Industry Brief (DNIB) reported 401.6 million domain name registrations across all top-level domains (TLDs) in Q2 2026, an 8.1% increase over Q2 2025. That figure reflects overall domain growth and not fraud domains specifically, but highlights the scale defenders are working against. At this volume, spotting a single lookalike domain before it is weaponized requires automated monitoring.

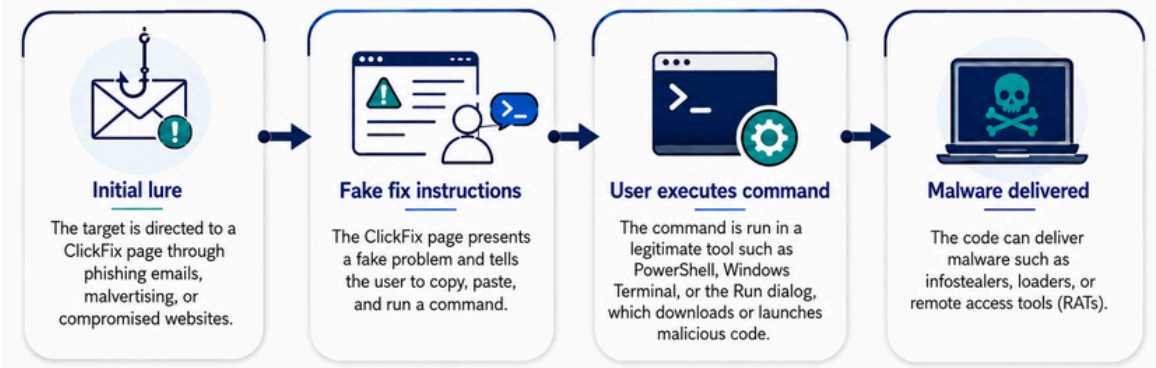


CLICKFIX: EVOLVING SOCIAL ENGINEERING

ClickFix has gone from a niche technique to one of the fastest-growing initial access methods in the threat landscape. What makes ClickFix worth calling out as a genuine trend, rather than a single clever gimmick, is who has adopted it and how fast it keeps evolving. This technique has been adopted by both state-backed and criminal actors. Nation-state groups have folded it into espionage operations, while ransomware operators use it as a reliable way to get a foothold before deploying ransomware or selling access to someone who will.

At its core, ClickFix turns the victim into the execution mechanism. Rather than exploiting a software vulnerability, attackers present a fake problem, such as a failed CAPTCHA, broken video player, or other seemingly routine technical problem, and then provide instructions for the user to "fix" it. Those instructions typically involve copying and pasting attacker-supplied commands into PowerShell, Windows Terminal, the Run dialog, or another legitimate system utility. Because the user initiates the command, the activity can bypass some traditional security controls and appear, at least initially, like legitimate administrative behavior.

EXAMPLE OF A TYPICAL CLICKFIX ATTACK CHAIN



ClickFix attacks have grown significantly. ESET recorded a 517% jump in ClickFix attacks from late 2024 through the first half of 2025, and detections rose another 108% in the first half of 2026. Food and agriculture organizations should consider incorporating these scenarios into security training. The fix is largely behavioral, since ClickFix relies on convincing a person to run a command, not on exploiting a technical vulnerability.

Food Ag-ISAC

Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC)

Launched in May 2023, the Food and Ag-ISAC provides 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.

Learn more at FoodAndAg-ISAC.org or email us at membership@foodandag-isac.org.