Food Ag-ISAC

2025 FOOD AND AGRICULTURE SECTOR CYBER THREAT REPORT

Powered by the Predictive Adversary Scoring System (PASS)

March 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.

Food Ag-ISAC

TABLE OF CONTENTS

INTRODUCTION

The Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC), built by and for the industry, monitors cyber threats targeting the food and agriculture sector and shares threat intelligence with member companies and partners to identify, prevent, mitigate, and respond to attacks. By collecting and sharing actionable intelligence and effective security measures, the Food and Ag-ISAC helps companies manage risk while strengthening resilience across the entire farm-to-table supply chain.

The following report examines the various cyber threat actors observed in the sector. The food and agriculture sector operates within a dynamic threat landscape where advanced nation-state actors and financially motivated cybercriminal groups continuously deploy sophisticated tactics, techniques, and procedures (TTPs). In this landscape, collaboration and shared intelligence are essential for anticipating adversary behavior and mitigating risks. *Defend Better. Defend Together.*

To advance these efforts, the Food and Ag-ISAC leverages the Predictive Adversary Scoring System (PASS) in partnership with member companies and the IT-ISAC. This tool helps prioritize the monitoring and analysis of known adversaries, enabling members to identify which threat actors pose the greatest danger to their organizations and the sector. By evaluating adversaries across multiple parameters, PASS enables organizations to quantify their susceptibility to specific threats and maximize their use of limited security resources.

PASS EXPLAINED

The Predictive Adversary Scoring System (PASS) provides a comprehensive scoring system based on specific factors, including the adversary's motivation, capabilities, and past actions, allowing organizations to assess their risk exposure and allocate resources accordingly.

PASS focuses on four key metrics to determine a specific adversarial risk:

- **Level of Activity:** How recently has the adversary been active.
- **Frequency of Sector Targeting:** The number of times the adversary has targeted the sector.
- **Sophistication/Impact:** The complexity of the adversary's tactics, techniques, and procedures (TTPs) and their impact.
- **Motivation:** The driving force behind the adversary: financial, geopolitical, ideological, or recognitional.

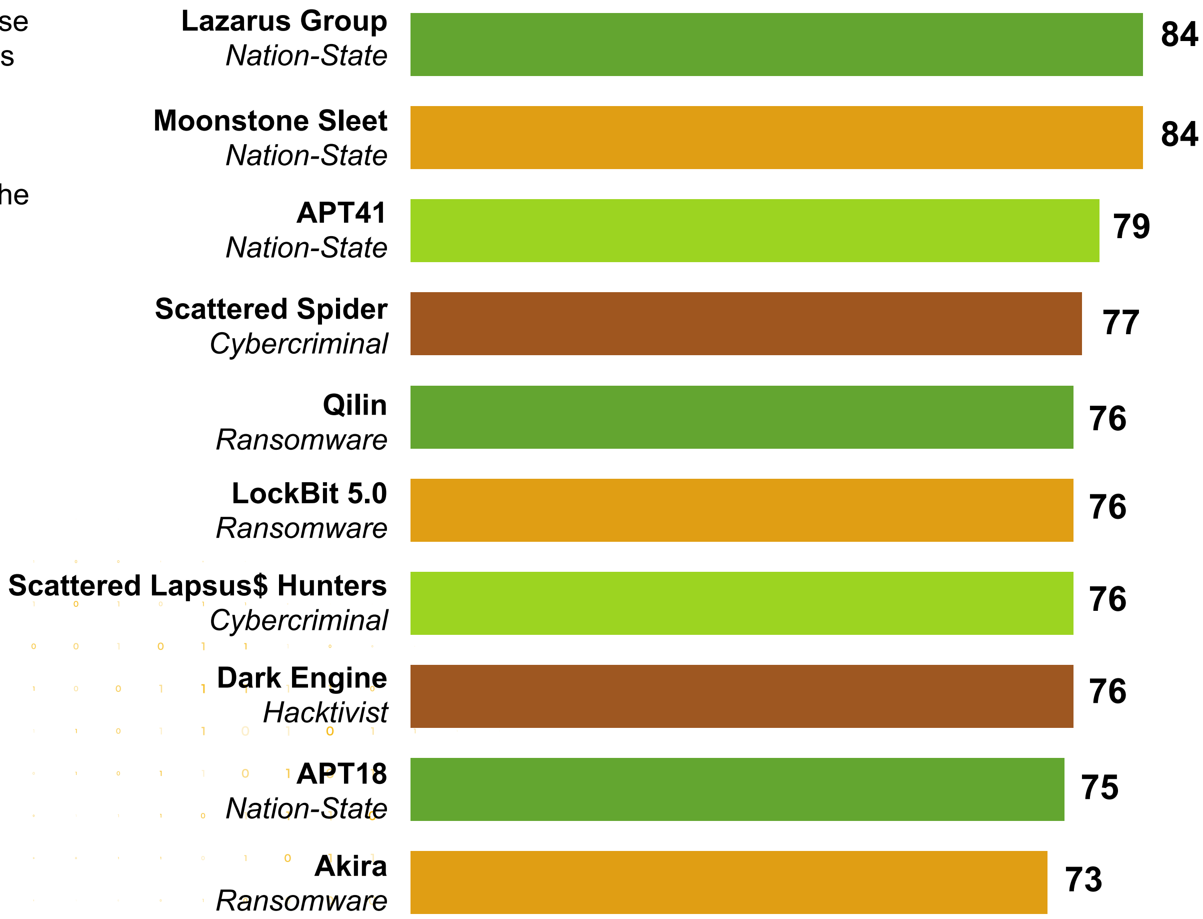
PASS employs a comprehensive set of metrics to assign adversaries a score ranging from 0 to 100, representing the highest level of threat when a threat actor satisfies all predefined system criteria. Higher scores indicate a greater risk to organizations within the sector. Adversaries with elevated scores represent significant threats due to their frequent targeting of the sector and their demonstrated sophistication and impact in past operations.

PASS is available to Food and Ag-ISAC members and is one tool in the suite of capabilities the ISAC uses to equip its members with actionable threat intelligence that advances their resilience and preparedness in an evolving threat landscape.

TOP 10 THREAT ACTORS

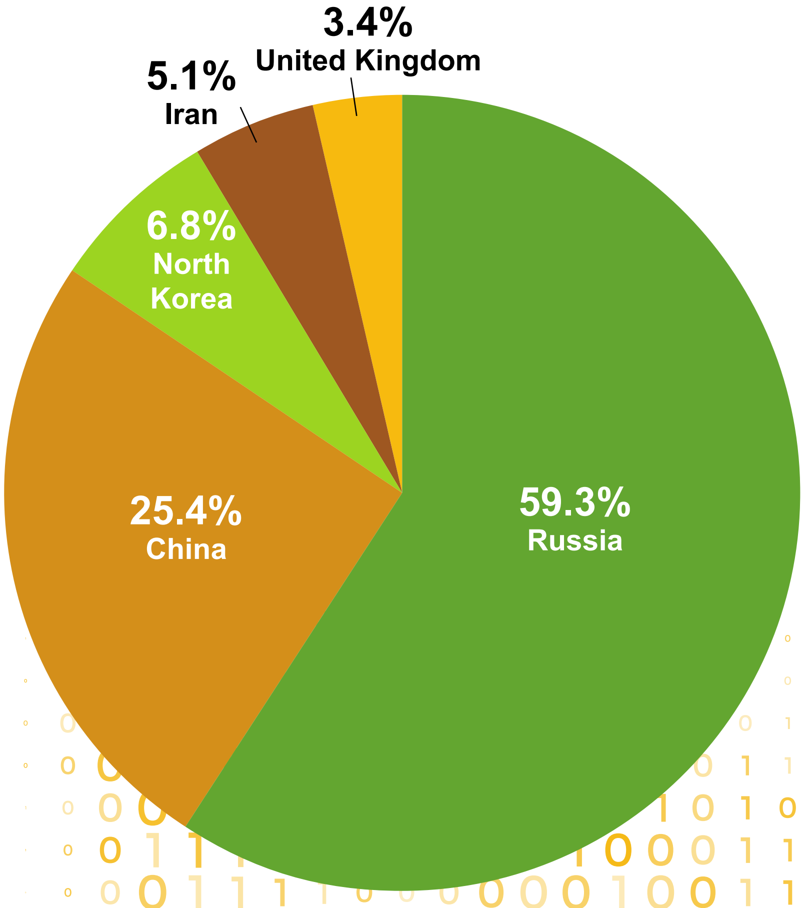
The Food and Ag-ISAC's analysts monitored over 330 adversaries as part of their broader threat landscape assessment. PASS was applied to these to identify and prioritize the adversaries most frequently observed in the food and agriculture sector. Through this comprehensive effort, 72 adversaries were identified as being active within the sector in 2025.

TOP 10 ACTORS PASS SCORE



SUMMARY OF ADVERSARY COUNTRY OF ORIGIN

ADVERSARY ORIGINS

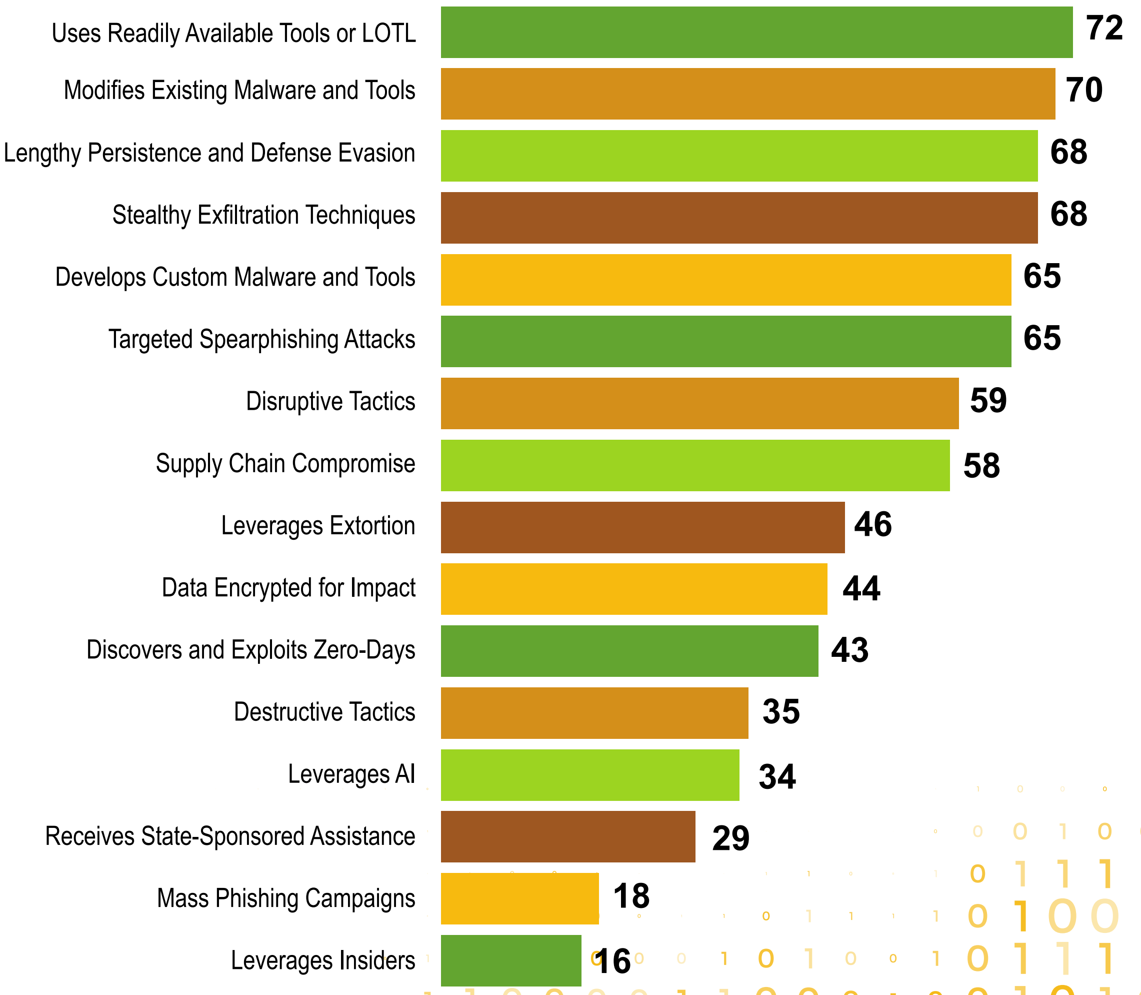


Russia had the highest concentration of adversaries observed in the food and agriculture sector in 2025. This is largely due to a majority of ransomware operations occurring in the region, out of reach of Western law enforcement. Indictments against a Russian adversary rarely lead to an arrest unless the individual travels to a country with a U.S. extradition treaty. Ransomware operators account for the majority of Russian-based activity observed in the sector, though Russia also maintains an active contingent of nation-state threat actors with a demonstrated presence within the food and agriculture sector.

China ranked second in terms of nations targeting the sector. China has a long history of targeting food and agriculture largely because of its interest in the sector's valuable intellectual property. The latest reports on long-term pre-positioning are ones that Food and Ag-ISAC analysts will continue to watch closely. While reports of just-in-case malware being found on food and agriculture sector networks are scarce, the sector would be a valuable target during geopolitical conflicts.

SUMMARY OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) USED BY ADVERSARIES

SOPHISTICATION TECHNIQUE (PASS COUNT)



MITIGATIONS

The mitigations below address tactics observed across the sector in 2025. Organizations should prioritize mitigations based on their current security maturity and threat exposure, recognizing that even incremental improvements can reduce risk.

- Multi-factor authentication (MFA) should be enabled wherever possible across all products and services. MFA relies on something you know (password) and something you have, typically a code sent to your physical mobile device, or a hardware token. This additional factor makes it much more difficult for adversaries to gain initial access to your account, even if your password is discovered. While mobile authenticators and hardware tokens are safer, any form of MFA, even SMS codes sent to your phone, is better than having nothing at all.
- Implement application whitelisting to restrict the execution of unauthorized binaries and scripts. This can be paired with the enhanced monitoring and logging of native tool abuse.
- Deploy behavior-based endpoint detection and response (EDR) solutions rather than relying on signature-based detection, since modified tools can easily bypass static signatures.
- Threat actors continue to target operational technology (OT) and industrial control systems (ICS). It is more common for adversaries to target your IT systems (email, workstations, SaSS platforms) first, before moving laterally to OT environments. Network segmentation can protect your more critical OT assets in the event that your IT systems are compromised.
- Enforce the principle of least privilege, regularly audit scheduled tasks, and conduct regular credential rotation and privilege reviews to disrupt long-dwell attackers.
- Deploy data loss prevention (DLP) solutions and monitor for anomalous outbound data volumes, including DNS tunneling and encrypted channels, using network traffic analysis (NTA) and full packet capture.
- Protect against phishing by continuously training users to spot spearphishing indicators and social engineering attempts (which often prey on unexpected urgency), as well as requests that bypass normal processes or communications that are convincing but slightly off.
- Maintain tested offline backups and incident response playbooks for destructive attack scenarios, including network segmentation to limit the blast radius.
- Establish a cyber incident response plan that includes coordination with legal, communications, and cyber insurance; never rely solely on ransom payment as a recovery strategy — having restorable backups is essential.

The 2025 threat landscape confirms that adversaries targeting the food and agriculture sector are persistent, adaptive, and not going anywhere. With 72 active threat actors identified across the sector, the case for collective defense has never been stronger. The threat landscape is too complex for any company to go at it alone. The Food and Ag-ISAC is committed to helping our members and the sector at large be secure and resilient. We will continue to provide a trusted forum for members to collaborate with peers, engage with subject-matter experts, and receive timely threat intelligence curated to the needs of food and agriculture companies. The strongest defense in any sector is collective: *Defend Better. Defend Together.*

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

🌐 FoodandAg-ISAC.org

✉ Membership@FoodandAg-ISAC.org