2025 IT SECTOR CYBER THREAT REPORT

March 2026

Powered by the Predictive Adversary Scoring System (PASS)

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

ABOUT THE IT-ISAC

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that provides a trusted forum for IT companies and those that leverage IT for core business functions to share information, manage risks, and collaborate on cyber incident response and strategy.

Our mission is to grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity, to serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies and practices for the benefit of all.

Our membership is comprised of security leaders from leading technology companies across the globe. We have built a network of relationships with trusted partners across the critical-infrastructure community and through this multidirectional sharing, we help companies manage risks to their enterprises and to the critical infrastructure community.

TABLE OF CONTENTS

INTRODUCTION

The Information Technology - Information Sharing and Analysis Center (IT-ISAC) plays a critical role in monitoring cyber threats targeting the IT sector, enabling member companies and partners to identify, prevent, mitigate, and respond to industry-targeted attacks through collaborative threat intelligence. By facilitating the collection, analysis, and dissemination of actionable intelligence and effective security measures, IT-ISAC helps members manage risk while strengthening resilience across the entire critical infrastructure ecosystem.

This report examines the various cyber threat actors observed in the sector and reflects IT-ISAC's core mission: equipping members with the insights and resources needed to counter sophisticated, active threats. The threat intelligence landscape is dynamic and evolving, with advanced nation-state actors and well-coordinated, financially motivated cybercriminal groups continuously deploying sophisticated tactics, techniques, and procedures (TTPs). While focused on the IT sector, this report also highlights interconnected risks affecting multiple industries – a crucial reminder that no sector operates in isolation.

The IT-ISAC maintains attack playbooks on more than 330 adversaries. These playbooks capture essential adversary data such as motives, TTPs, and known sectors of operation. The IT-ISAC developed the Predictive Adversary Scoring System (PASS) in partnership with member organizations to prioritize the monitoring and analysis of known adversaries. PASS enables us to identify which threat actors present the greatest danger to specific sectors and sub-sectors. This helps members understand which threat actors are most relevant to them. By evaluating adversaries across multiple parameters including capability, intent, and historical activity, PASS allows organizations to quantify their susceptibility and make informed resource allocation decisions.

PREDICTIVE ADVERSARY SCORING SYSTEM (PASS) EXPLAINED

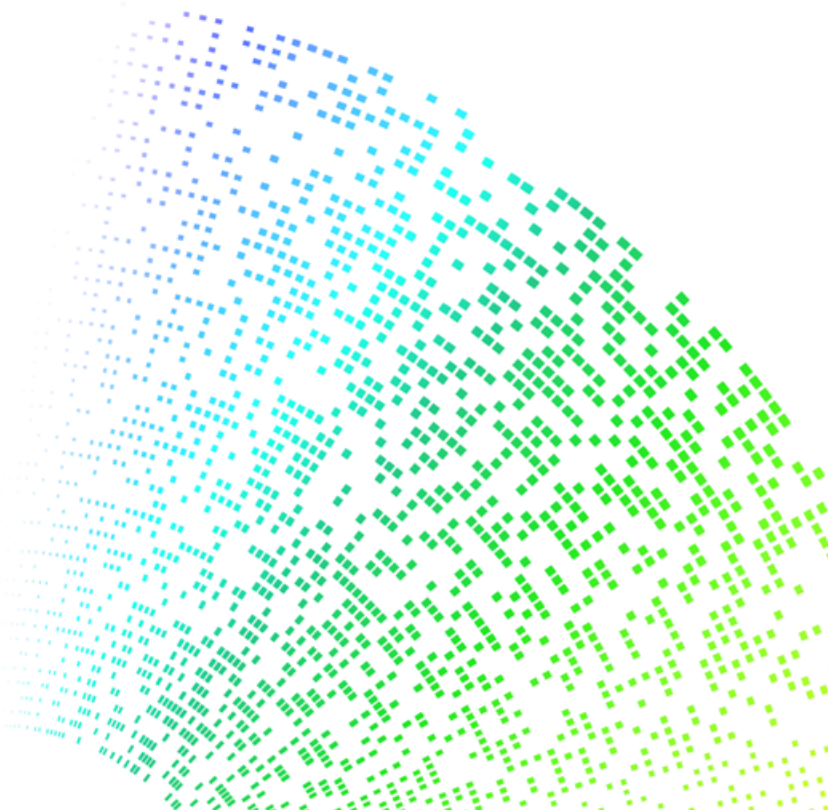
The Predictive Adversary Scoring System (PASS) provides a comprehensive scoring system based on specific factors, including the adversary's motivation, capabilities, and past actions, allowing organizations to assess their risk exposure and allocate resources accordingly.

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 IT 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.

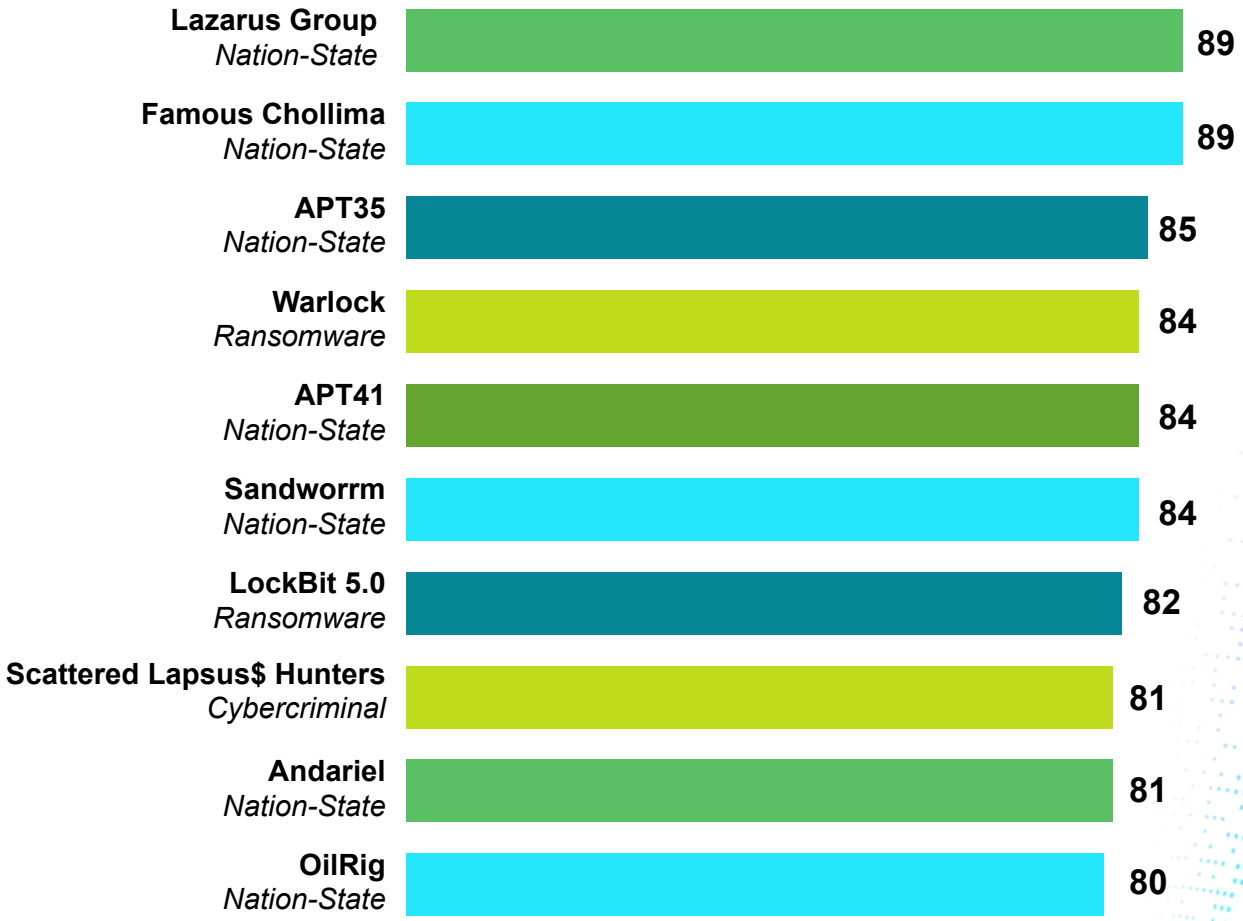
PASS is available to Food and Ag-ISAC members in Excel and Google Sheet versions for easy data entry and analysis. Members leveraging PASS gain valuable insights into the threats they face, enabling them to improve their defenses or prepare for an impending attack. This tool facilitates the ISAC's ongoing mission to equip its members with actionable capabilities that advance their resilience and preparedness in an evolving threat landscape.



TOP 10 THREAT ACTORS | IT SECTOR

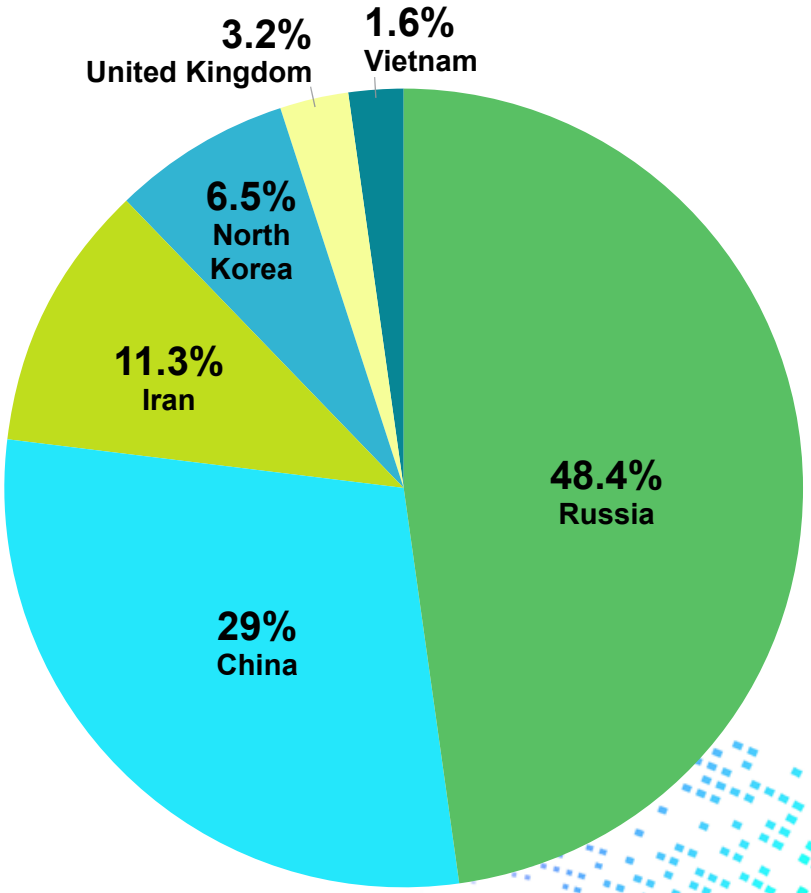
PASS was applied to the over 330 Adversary Attack Playbooks the IT-ISAC maintains to identify and prioritize the adversaries most frequently targeting the IT industry. This comprehensive effort identified 77 adversaries active in the IT Sector in 2025. Below, we have highlighted the top 10 adversaries targeting the IT Sector.

TOP 10 ACTORS PASS SCORE



SUMMARY OF ADVERSARY COUNTRY OF ORIGIN

ADVERSARY ORIGINS, EXCLUDING N/A



Please note this excludes adversaries not associated with a country of origin.

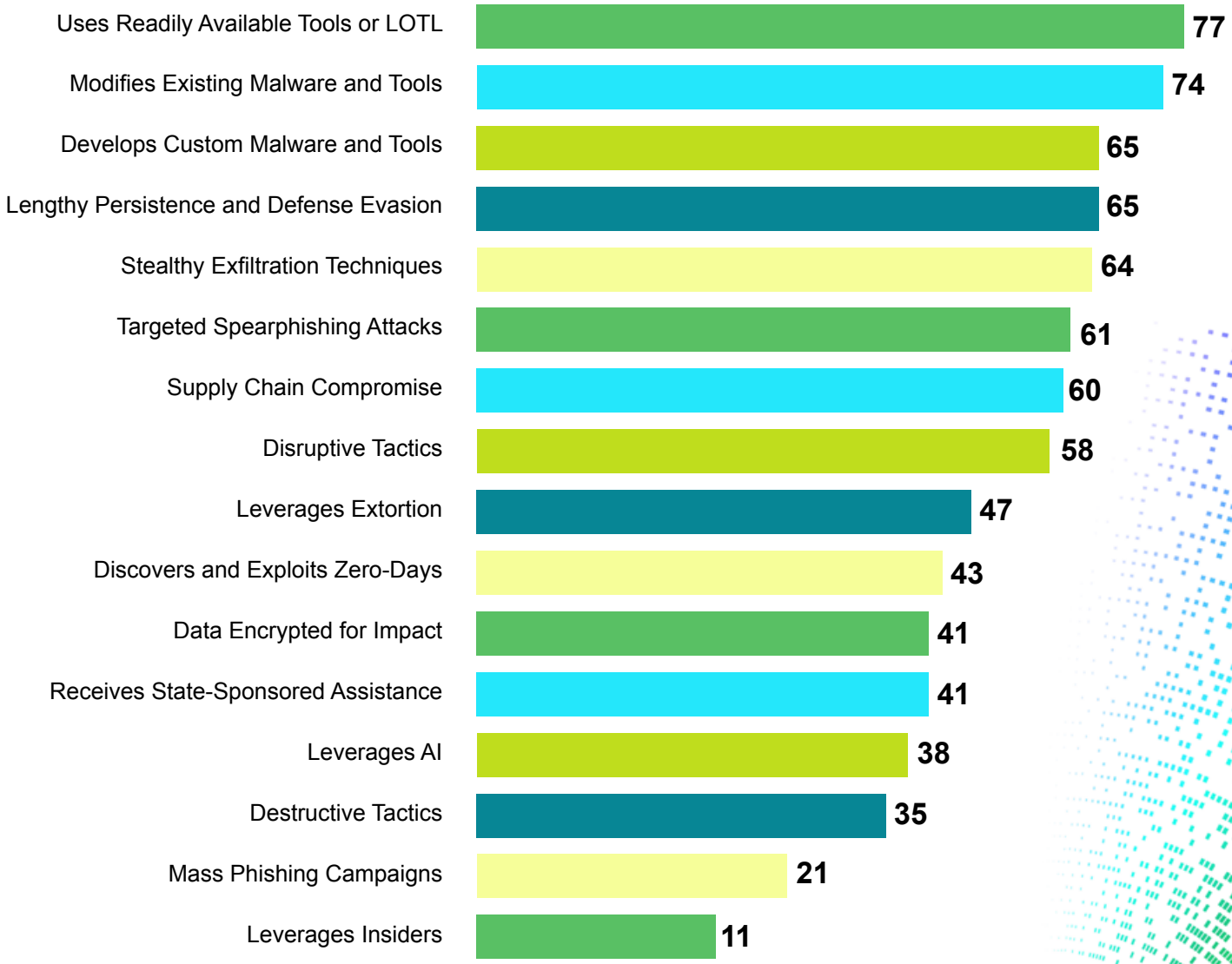
There is a wide range of cyber groups operating from or linked to Russia, including ransomware gangs, financially motivated cybercriminals, hacktivist collectives, and state-affiliated actors. In fact, 48.4% of all observed threat actors active against the sector in 2025 originated in Russia. These groups targeted IT companies for different reasons: some focused on making money through ransomware or selling stolen access, while others pursued espionage or disruptive activity tied to broader geopolitical tensions.

China ranked second among countries with the most actors targeting the IT sector, accounting for 29% of the total. Chinese adversaries have historically focused on intellectual property theft and cyber espionage. However, in recent years, these actors have increasingly prioritized long-term persistence across critical infrastructure, including within telecommunications networks, cloud environments, and other critical digital infrastructure, allowing them to maintain continuous access, monitor systems, and gather intelligence over extended periods.

Actors from Iran, North Korea, the United Kingdom, and Vietnam represented smaller portions of the overall landscape. Iranian groups (11.3%) continued to conduct espionage and disruptive cyber operations aligned with regional and political tensions. Whereas, North Korean actors (6.5%) remained heavily focused on revenue generation, including cryptocurrency theft and fraudulent remote IT worker schemes.

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

SOPHISTICATION TECHNIQUE (PASS COUNT)

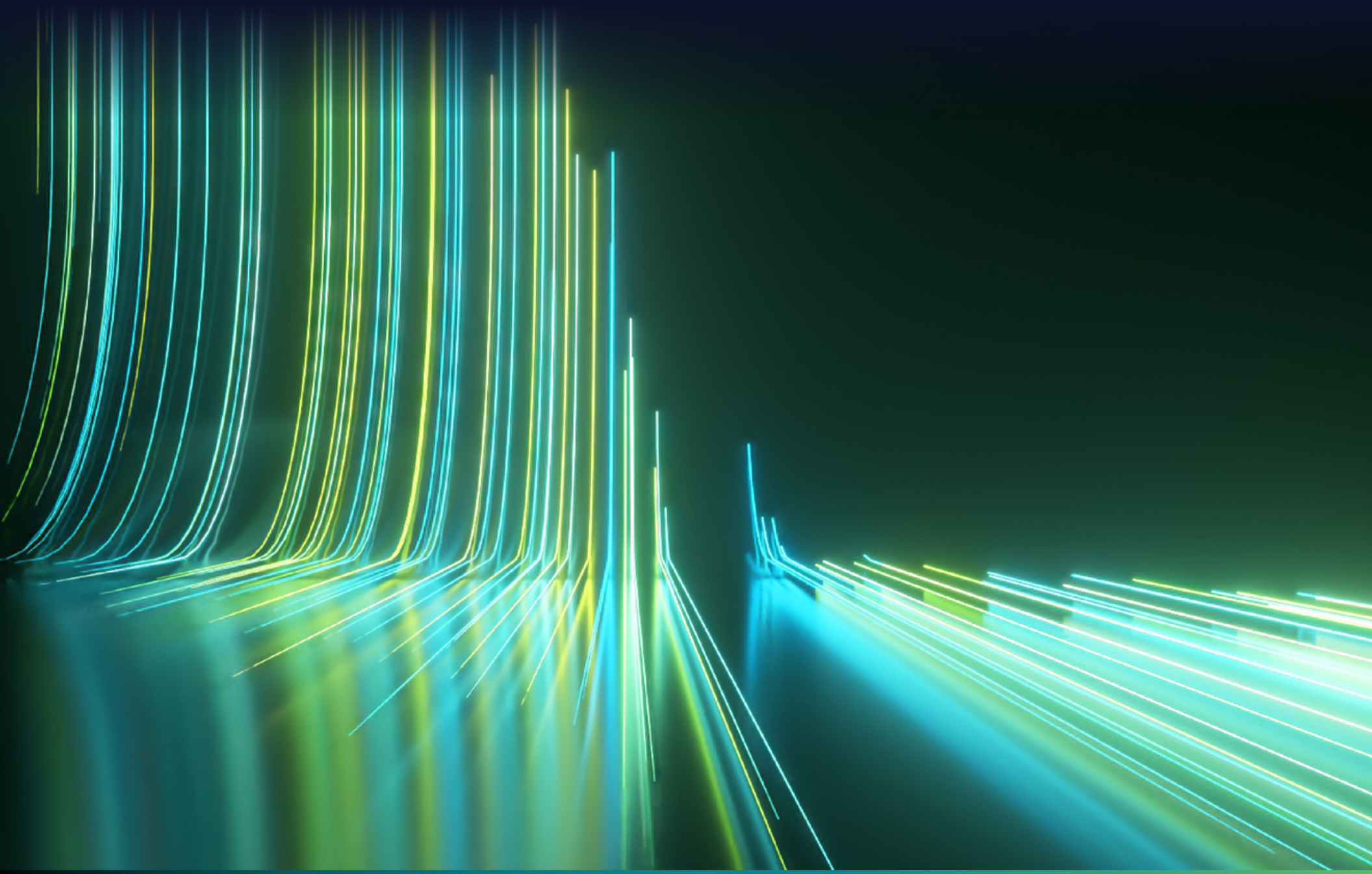


MITIGATIONS

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.*



The attackers share with each other.
The defenders share with us.

IT-ISAC.org
Membership@IT-ISAC.org