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

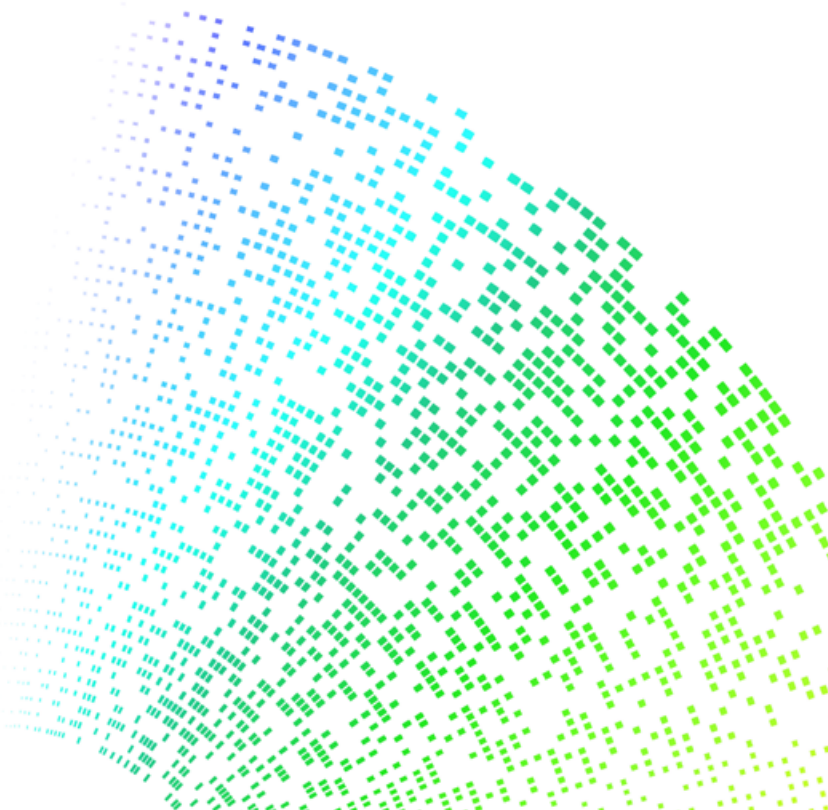
The Predictive Adversary Scoring System (PASS) provides a comprehensive scoring system based on specific factors, including the adversary's motivation, capabilities, and past actions, allowing organizations to assess their risk exposure and allocate resources accordingly.

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.

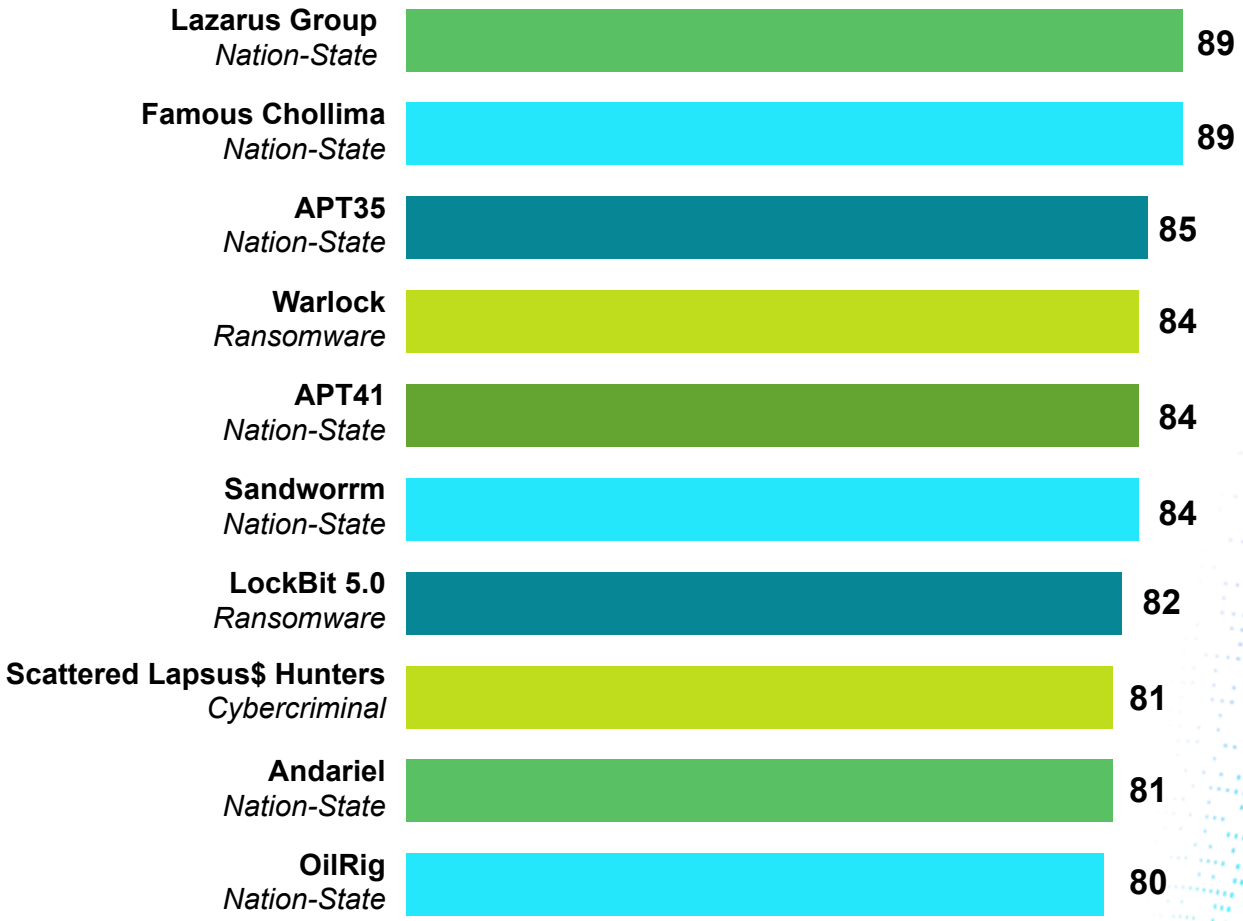
PASS is available to IT-ISAC members and is one tool in the suite of capabilities the ISAC uses to equip its members with actionable threat intelligence that advances their resilience and preparedness in an evolving threat landscape.



TOP 10 THREAT ACTORS | IT SECTOR

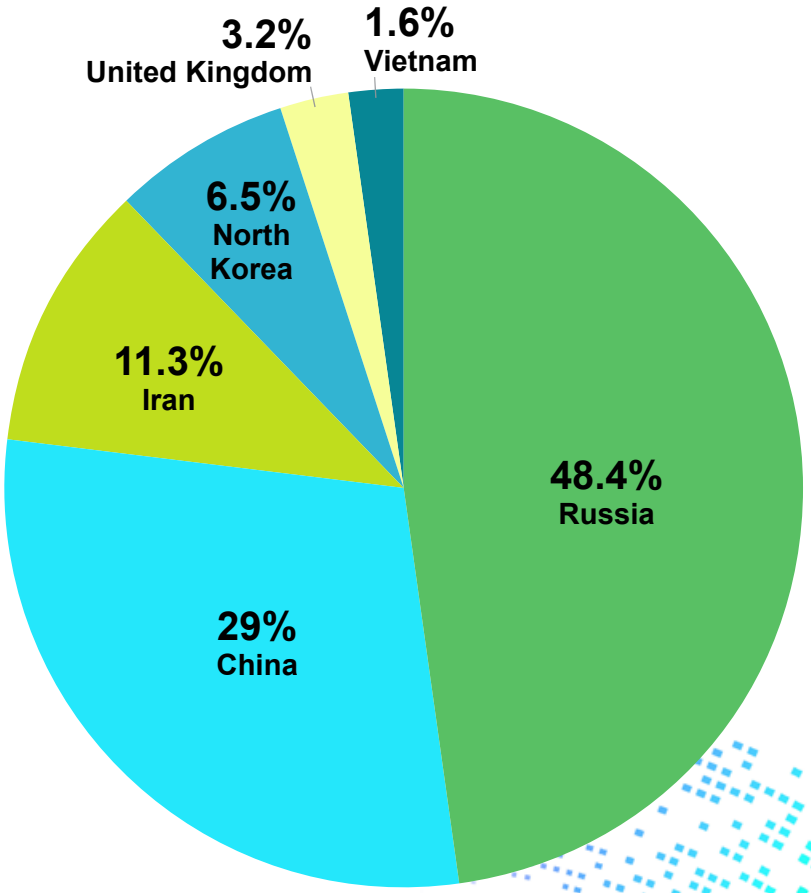
PASS was applied to the over 330 Adversary Attack Playbooks the IT-ISAC maintains to identify and prioritize the adversaries most frequently targeting the IT industry. This comprehensive effort identified 77 adversaries active in the IT Sector in 2025. Below, we have highlighted the top 10 adversaries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

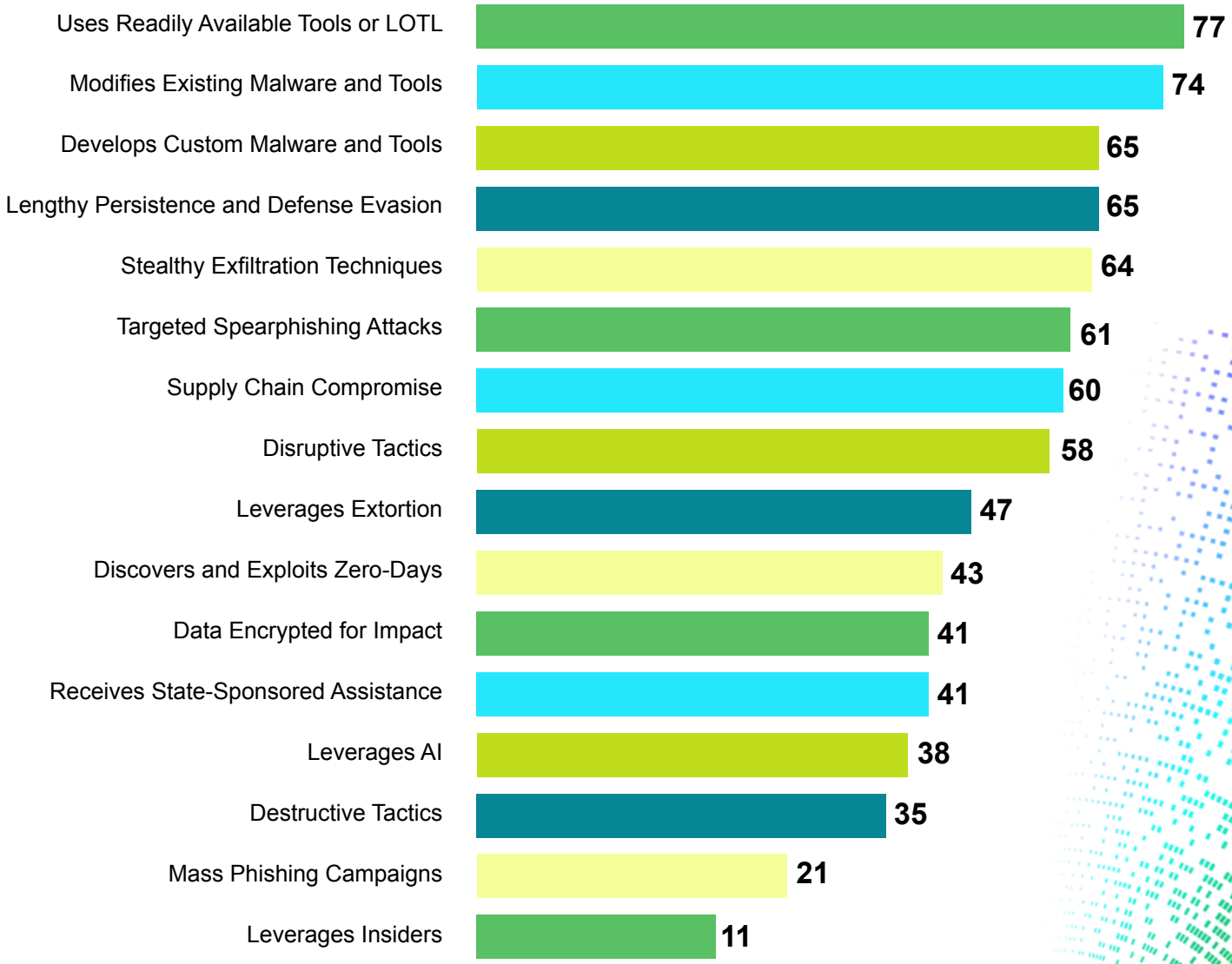
There is a wide range of cyber groups operating from or linked to Russia, including ransomware gangs, financially motivated cybercriminals, hacktivist collectives, and state-affiliated actors. In fact, 48.4% of all observed threat actors active against the sector in 2025 originated in Russia. These groups 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)

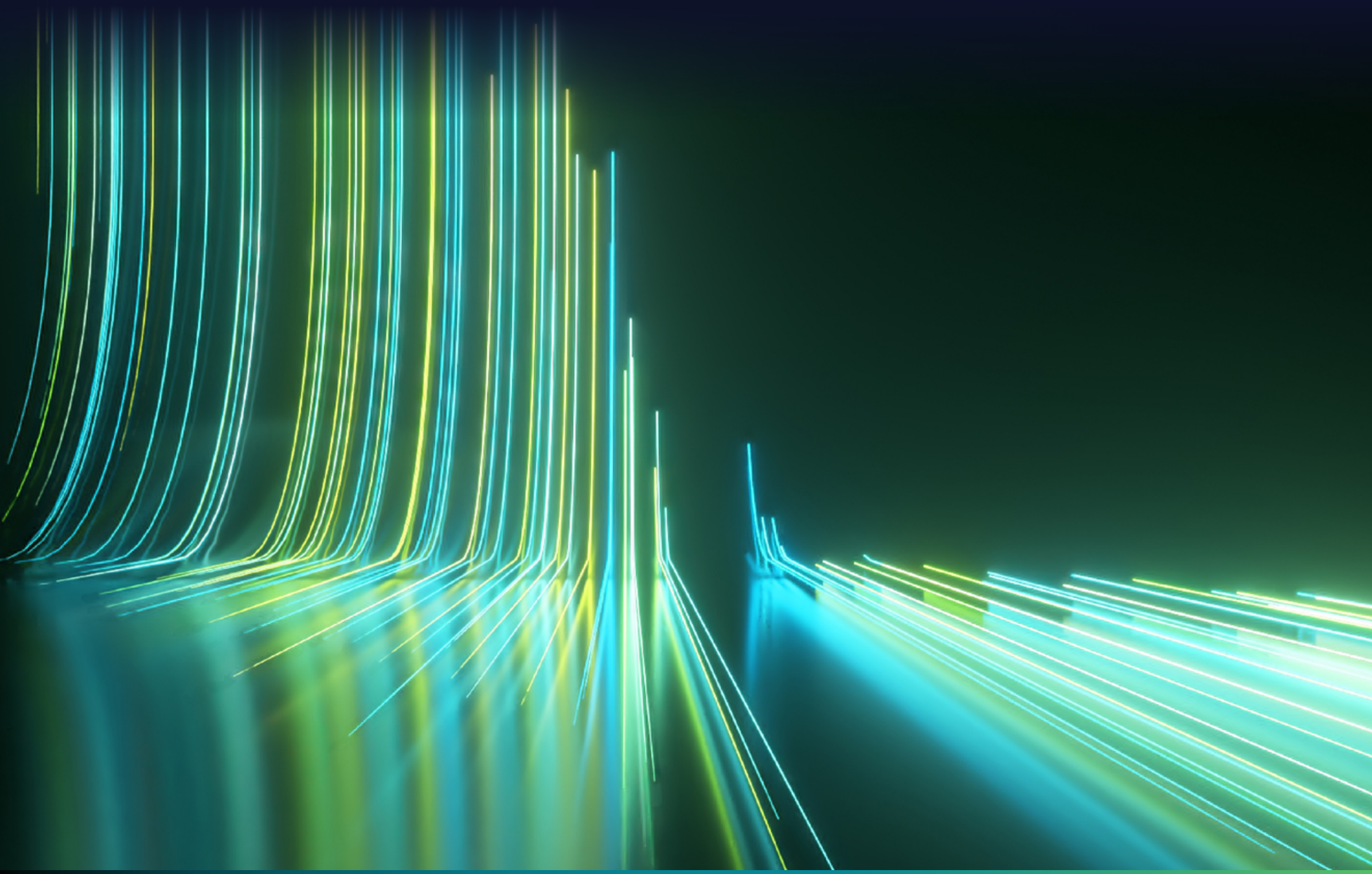


MITIGATIONS

The 2025 threat landscape was defined by volume, variety, and persistence. Across 77 active adversaries, the IT sector faced nation-state espionage, ransomware campaigns, supply chain infiltration, and extortion. Adversaries are patient, resourceful, and increasingly sophisticated; there are steps companies can take to defend themselves. The following mitigations address specific tactics documented in this report and offer a practical starting point for organizations at every stage of their security journey.

- The first line of defense is your employees - security awareness training can help employees stop incidents before they occur.
- Organizations should implement multi-factor authentication (MFA) wherever possible. Pairing traditional passwords with an additional factor can lessen the chance of an adversary gaining access to your systems and services. Any MFA is better than none — but not all MFA is equal. Mobile authenticator apps are generally more secure than SMS-based codes, and organizations can deploy phishing-resistant options like hardware tokens (FIDO2) or biometric authentication (face, fingerprints, etc.).
- Baseline and monitor native system tools (PowerShell, WMI, certutil) for anomalous usage patterns. Restrict execution where operationally feasible using application allowlisting.
- Deploy behavioral analytics and heuristic-based EDR to detect tools that have been modified to evade signature-based detection.
- Focus defenses on behavior, not binaries. Anomalous process creation, unusual network beaconing, and unexpected privilege escalation are red flags regardless of whether the tool has ever been seen before.
- Implement centralized logging with extended retention and conduct regular threat hunting. Assume there is a breach and look for low-and-slow lateral movement rather than waiting for an alert to fire.
- Monitor outbound traffic for anomalies in volume, timing, and destination. Enforce DLP controls and analyze metadata from encrypted traffic when full inspection is not possible.
- Layer email authentication controls (DMARC) with technical protections such as attachment sandboxing and URL rewriting, combined with regular, role-specific phishing training and simulations.
- Vet third-party software and service providers rigorously and enforce least-privilege access for all vendor connections. Monitor for unexpected behavior in trusted software and enforce integrity verification where possible, such as code-signing validation.
- Segment your IT and OT environments. 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, SaaS platforms) first before moving laterally into OT environments.
- Develop and regularly exercise incident response and business continuity plans. Segment critical systems and maintain tested, offline backups so disruption doesn't become destruction.
- Never treat ransom payment as a recovery strategy. Invest in resilience and a clear internal escalation protocol so panic doesn't drive the response.
- Implement compensating controls such as network segmentation, least privilege, and EDR behavioral monitoring that catches exploitation attempts even for unknown vulnerabilities.

Organizations do not have to face these threats alone. Joining an information-sharing community like the IT-ISAC opens access to a trusted network of peers navigating the same threat landscape. Members receive real-time threat intelligence, early warning on emerging threats and zero-day vulnerabilities, and the opportunity to collaborate directly with analysts and security teams across the sector. In cybersecurity, shared knowledge isn't just an advantage; it's a force multiplier.



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

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