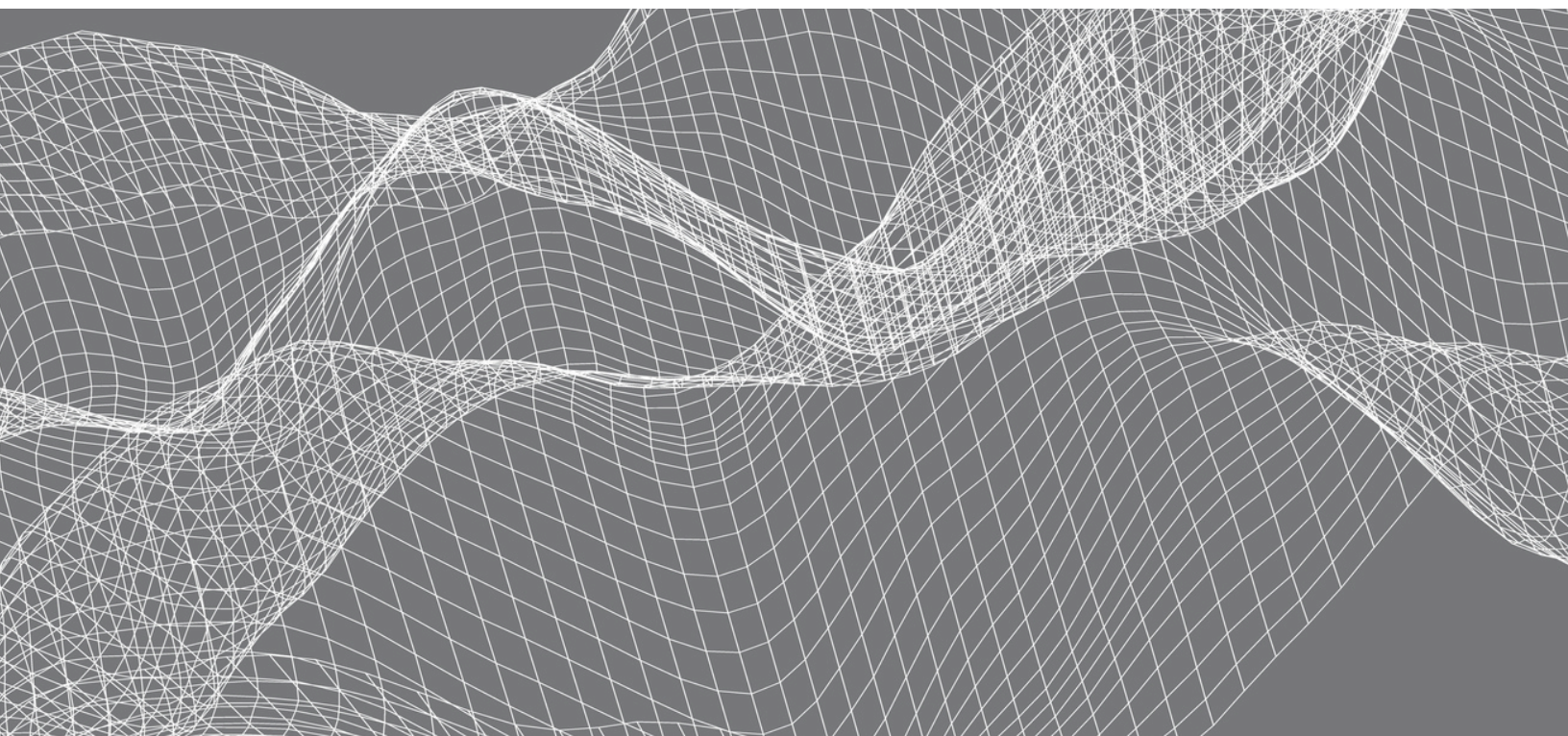




IT Sector Cyber Threat Report

MARCH 2025



INTRODUCTION

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments its member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies. Our members are committed to cybersecurity and serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat intelligence, effective security policies, and practices for the benefit of all. Attackers share with each other. Defenders share with us.

The IT-ISAC recently created the Predictive Adversary Scoring System (PASS) in collaboration with its member companies to help prioritize the monitoring and analysis of known adversaries. This tool enables us to identify threat actors that pose the greatest danger to entities facing the industry, such as specific state-sponsored actors or cybercrime syndicates. PASS provides a comprehensive scoring system based on various factors, including the adversary's motivation, capabilities, and past actions, allowing members to assess their risk exposure and allocate resources accordingly.

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

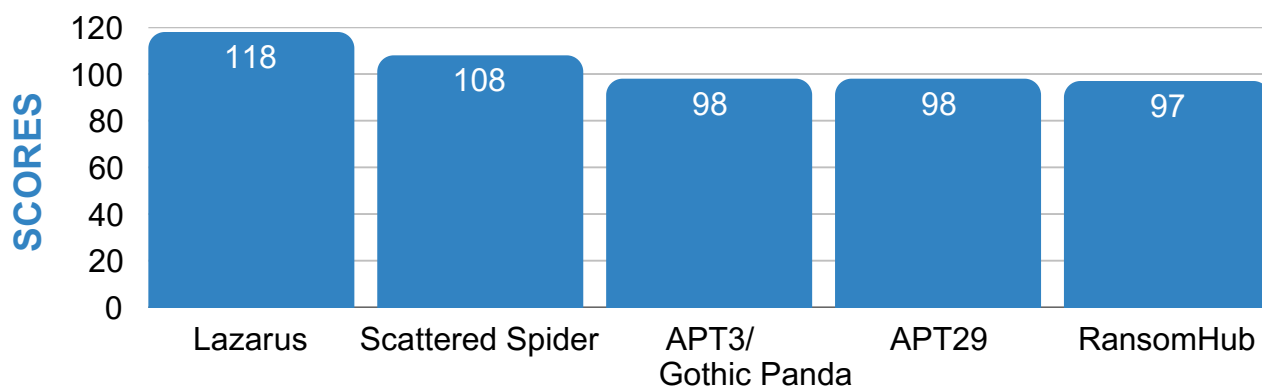
- ✓ **Level of Activity:** How recently has the adversary been active.
- ✓ **Frequency of Sector Targeting:** The number of times the adversary has targeted the IT sector.
- ✓ **Sophistication/Impact:** The complexity of the adversary's tactics, techniques, and procedures (TTPs) and their impact.
- ✓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

To produce this report, IT-ISAC members contributed lists of threat actors known to have historically targeted the IT sector. Building on these contributions, the IT-ISAC's analysts monitored over 230 adversaries as part of their broader threat landscape assessment. Using the PASS system, a structured methodology was applied to identify and prioritize the adversaries most frequently targeting the IT industry. This comprehensive effort narrowed the focus to 59 adversaries, which the IT-ISAC's operations team analyzed in detail. The full report is available to IT-ISAC members, with high-level insights outlined below.

TOP 5 THREAT ACTORS

The PASS system employs a comprehensive set of metrics to assign adversaries a score ranging from 0 to a maximum of 128, representing the highest level of threat achieved when a threat actor satisfies all of the system's predefined criteria. The higher scores indicate a greater level of 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.

The top 5 threat actors identified were Lazarus, Scattered Spider, APT3/Gothic Panda, APT29, and RansomHub.



SUMMARY OF THREAT ACTOR MOTIVATION

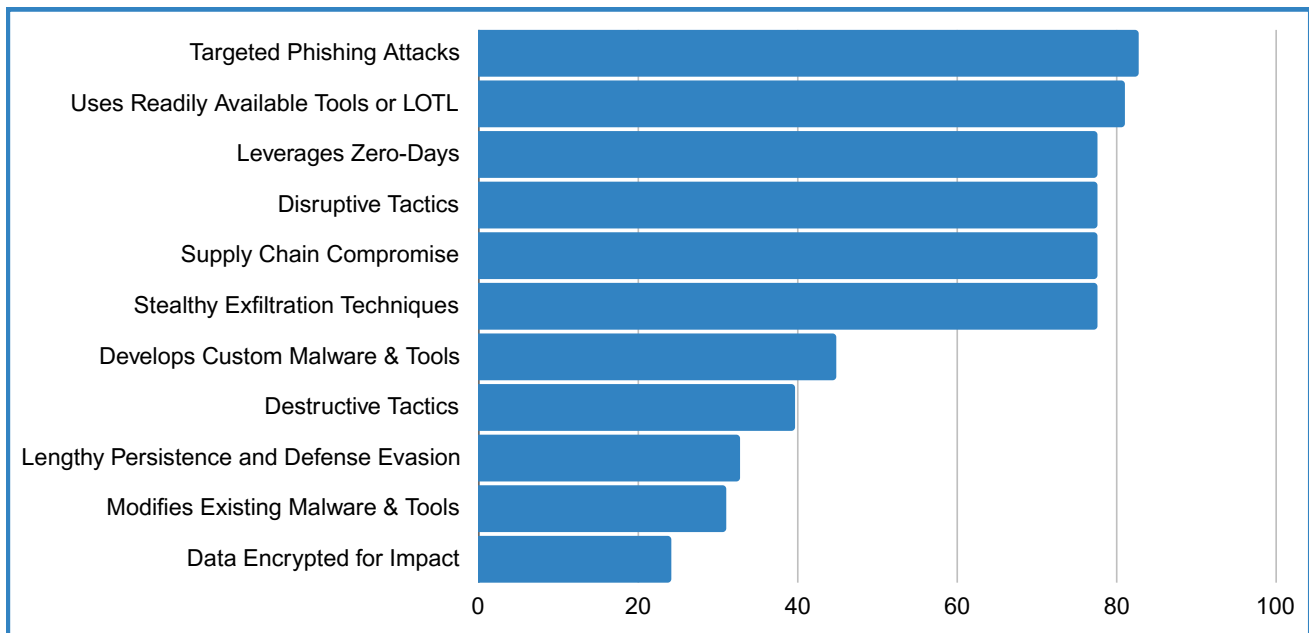
The PASS scoring system reveals that attacks against the IT sector are split between 52% geopolitically driven and 48% financially motivated. Geopolitical attacks typically aim to disrupt operations, steal sensitive information, or weaken competitors, often as part of a broader state-sponsored agenda. In contrast, financially motivated ransomware groups focus on extortion, leveraging tactics such as data exfiltration and system encryption to demand payouts. The IT sector's diverse range of targets, troves of intellectual property and sensitive data, operational dependency, interconnected networks, and critical high-value digital infrastructure make it a prime focus for geopolitical and financial attackers.



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

To produce this report, IT-ISAC members contributed lists of threat actors known to have historically targeted the IT sector. Building on these contributions, the IT-ISAC's analysts monitored over 230 adversaries as part of their broader threat landscape assessment. Using the PASS system, a structured methodology was applied to identify and prioritize the adversaries most frequently targeting the IT industry. This comprehensive effort narrowed the focus to 58 adversaries, which the IT-ISAC's operations team analyzed in detail. Through this analysis, we identified the top tactics, techniques, and procedures (TTPs) used by adversaries most frequently seen in the IT sector.

Percentage of Threat Actor TTPs




RISK MITIGATIONS

Companies should focus on allocating their limited resources to maximum effect. Implementing informed risk management strategies help companies prioritize security investments and practices. An organization may decide to accept a risk today with the goal of reducing the risk in the future - no risk acceptance should be finite and decisions should be re-evaluated at regular intervals. A key part of risk management is to ensure you are constantly reviewing the threat environment and investment decisions. While informed risk management will help companies reduce their risk exposure, the risk will never be eliminated.

Based on our research and insights of threat actors, we believe the following mitigations are effective practices for defending against observed adversaries. This list is not all-encompassing, and implementing them does not guarantee that organizations will not be breached. However, these practices can bolster defenses against the TTPs highlighted above.


Train Employees to:


- Not open emails or download software from untrusted sources – verify the domain even if it seems like a legitimate software hosting site.
- Not click on links or attachments in emails that come from unknown senders.
- Not provide passwords, personal information, or financial information via email to anyone (sensitive information is also used for double extortion).
- Always verify the email sender's email address, name, and domain.
- Report phishing emails to appropriate security or IT staff immediately.

 **Consult and apply vendor-recommended guidance for security hardening.** To the extent possible, enable security features at the highest possible setting.

 **Implement application allowlisting and monitor the use of common LOLBins.** (*Living off the Land Binaries – trusted, pre-installed system tools used to spread malware and carry out their work*)

 **Review CISA Guidance on [Living Off the Land \(LOTL\) Techniques Mitigation](#).**

 **Ensure access to timely and relevant cyber threat intelligence.** Stay updated by following cybersecurity publications, prominent researchers, and vendors on social media. Collaborate with industry peers.

 **Strengthen patch management.** Implement and keep under review robust processes for testing and applying patches as soon as possible.

- **Use advanced detection tools.** Behavioral and anomaly-based detection systems can help identify exploitation attempts, even for unknown vulnerabilities.
- **Mitigate network disruptions.** Implement robust cybersecurity measures such as network segmentation, intrusion detection systems (IDS), and regular vulnerability assessments. Additionally, a [recent joint advisory](#) on the dangers of nation-state actors released by CISA with the National Security Agency and the Federal Bureau of Investigation provides suggested mitigations.
- **Evaluate third-party risks.** Assess the risk management and cyber security practices of third-party partners and providers.
- **Implement least privilege access.** Limit the access and permissions granted to third parties, ensuring they only have access to resources essential for their role.
- **Enforce service control policies (SCPs).** For cloud-based resources, create policies that restrict roles or users across the organization from accessing specific services or performing sensitive actions.
- **Strengthen software vetting.** Establish rigorous review processes for open-source software and libraries, minimizing the risk of introducing compromised code into the development pipeline.
- **Implement multi-factor authentication (MFA).** External-facing assets that leverage single-factor authentication (SFA) are highly susceptible to brute-forcing attacks, password spraying, or unauthorized remote access using valid (stolen) credentials. [Implementing MFA](#) enhances security and adds an extra layer of protection.

Last but certainly not least, joining an information-sharing forum, such as the IT-ISAC, is a good way to stay up-to-date on the latest malware strains and to collaborate with peer organizations and individuals who are facing the same challenges. Companies can strengthen their cybersecurity strategies by sharing threat intelligence through [Information Sharing and Analysis Centers](#) (ISACs). By joining these centers, companies gain early insights into emerging threats and zero-day vulnerabilities. Additionally, companies have the opportunity to collaborate directly with analysts from peer companies, enabling proactive enhancement of their defenses.



ABOUT THE IT-ISAC

Founded in 2000, the **Information Technology - Information Sharing and Analysis Center** (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

We serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat intelligence, effective security policies, and practices for the benefit of all.

[IT-ISAC.ORG](https://www.it-isac.org)

MEMBERSHIP@IT-ISAC.ORG