DARKTRACE

ANNUAL THREAT REPORT 2026: AMERICAS (AMS) REGIONAL OUTLOOK

The global cyber threat landscape in 2025 was increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives. This regional breakdown provides a focused analysis of the key threat trends, notable threat actors, and outlook for the AMS region.

REGIONAL TRENDS AND STATISTICS

While these statistics and insights reflect trends across the broader Americas region, the majority of Darktrace customers in this market are based in the United States.

TOP ATTACK VECTORS

Software-as-a-Service (SaaS)/Microsoft 365 account compromise and phishing or email based social engineering account for nearly 70% of all recorded incidents, making credential abuse the single most effective initial access vector.

These incidents commonly involve malicious inbox rules, session hijacking, OAuth abuse, and thread hijacking highlighting attackers' preference for living-off-the-land (LOTL) techniques and exploiting trusted platforms.

While phishing remains a primary entry point, the impact phase is shifting sharply toward ransomware and data extortion. Ransomware incidents often followed earlier cases of credential compromise or VPN/edge exploitation.

Ransomware cases increasingly include pre-encryption data exfiltration, indicating a move away from pure encryption only attacks toward double extortion and data leak pressure tactics. This trend aligns with the rise of groups such as Akira, Qilin, and BlackSuit, which prioritize identity compromise, lateral movement, and data staging before execution.

TOP RANSOMWARE

The threat activity observed is dominated by financially-motivated ransomware and identity-focused cybercriminal groups. Akira is the most frequently identified actor, followed by Qilin. Additional activity linked to BlackSuit, Scattered Spider, Dire Wolf, and RansomHub highlights a landscape driven primarily by ransomware, extortion, and account compromise rather than nation-state espionage.

Social engineering-driven identity compromise is frequently followed by ransomware deployment or data leak extortion, reducing attacker dwell time and maximizing business impact. This trend reflects the continued maturation of ransomware ecosystems, with which access to theft, lateral movement, and monetization are often handled by distinct but cooperating threat groups.

The Manufacturing industry accounted for the largest share of recorded ransomware incidents in 2025, representing 29% of all cases. This was more than twice that of the next most impacted sector, Human Health and Social Work. The significant gap highlights Manufacturing's heightened exposure to operational disruptions and its attractiveness to threat actors targeting critical supply chains.

MOST IMPACTED SECTORS

Manufacturing is also the most impacted sector overall, accounting for 17% of all recorded incidents, followed by Construction, Public Administration and Defense, Healthcare, Financial Services, and Information and Communication.

Collectively, these sectors make up over half of all incidents within the region, highlighting adversaries' preference for environments with high operational criticality, regulatory exposure, and reliance on SaaS based identity systems. Targeting patterns indicate a clear shift toward operationally intensive and digitally transforming sectors. Manufacturing and Construction environments continue to experience elevated threat activity as increased digitization, third party access, and hybrid IT/Operational Technology (OT) models expand the attack surface.

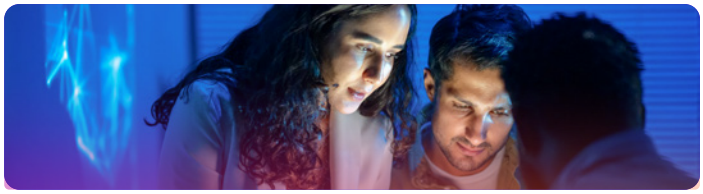
This trend suggests that mainstream and financially-motivated adversaries are increasingly prioritizing business impact and disrupting potential over sector-specific data sensitivity.

For the second year in a row, Manufacturing remains the most affected industry, recording the highest number of security incidents originating from this sector. This sustained trend underscores the sector's vulnerability, driven by its reliance on interconnected OT and legacy systems, which often lack robust security controls. The prevalence of attacks against Manufacturing highlights the critical need for enhanced cybersecurity measures, particularly as adversaries continue to exploit these environments for ransomware deployment, data exfiltration, and disruption of production processes.

REGIONAL VS. GLOBAL COMPARISON

The North America region—particularly the US—continues to be a persistent hotspot for cyberattacks due to its increasing digital dependence, rapidly expanding attack surface driven by widespread Internet of Things (IoT) adoption, and extensive critical-infrastructure footprint.

These factors make it an attractive target for both financially motivated cybercriminal groups and nation-state actors seeking disruption, espionage, or strategic advantage. This is reflected in the fact that nearly 47% of all security incidents observed in Darktrace cases globally in 2025 originated in the AMS region.

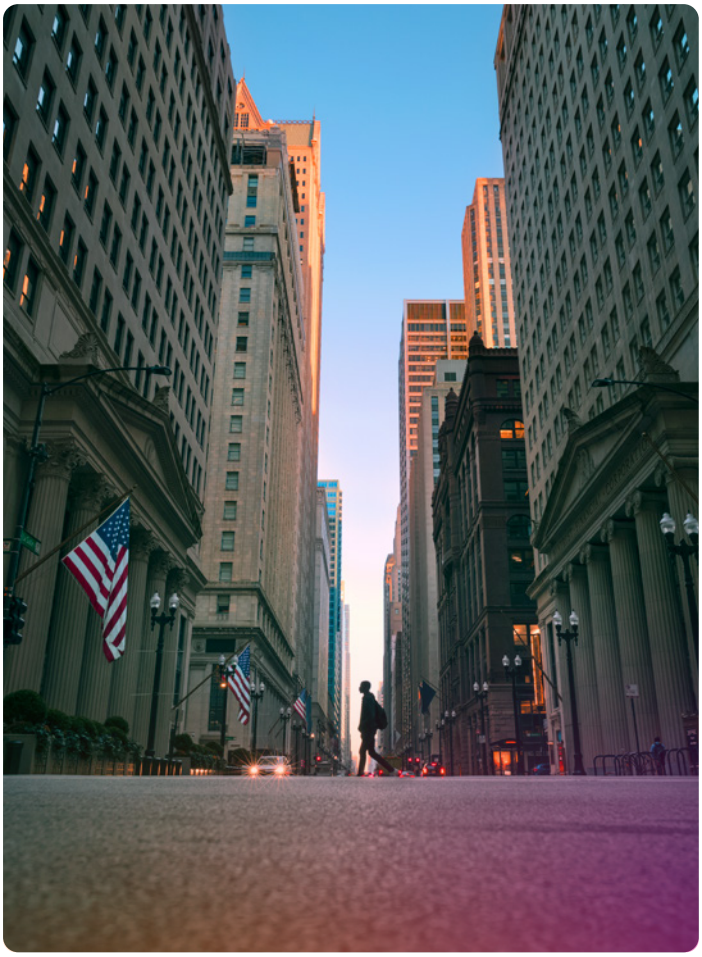


CASE STUDY

In May 2025, Darktrace investigations revealed attackers exploiting Ivanti infrastructure to gain access for malware deployment across multiple customers. These incidents highlight how exposed management and edge systems continue to provide attackers with trusted footholds when remediation is delayed or incomplete.

NOTABLE THREAT ACTORS

Actor	Motivation & Targets	Key Tactics
Scattered Spider	**Scattered Spider is a native English-speaking cybercriminal group active since at least 2022,** initially targeting Business Process Outsourcing (BPO), Telecommunications, and Technology organizations before expanding into the gaming, Hospitality, Retail, MSP, Manufacturing, and Financial sectors. The group relies heavily on social engineering, most notably help-desk impersonation and multi-factor authentication (MFA)-bypass techniques, to obtain high-privilege access across hybrid cloud and identity environments such as Okta, Amazon Web Services (AWS), and Microsoft 365. Scattered Spider continuously evolves its tooling to evade Endpoint Detection and Response (EDR) controls and support ransomware-driven financial operations.	**Reconnaissance** - T1598 - Phishing for Information **Initial Access** - T1566 – Phishing **Execution** - T1204 - User Execution **Privilege Escalation** - T1068 - Exploitation for Privilege Escalation **Defense Evasion** - T1656 - Impersonation **Credential Access** - T1621 - Multi-Factor Authentication Request Generation **Lateral Movement** - T1021 - Remote Services **Command and Control** - T1102 - Web Service **Command and Control** - T1219 - Remote Access Tools **Command and Control** - T1572 - Protocol Tunneling **Exfiltration - T1567** - Exfiltration Over Web Service **Impact** - T1657 - Financial Theft
Akira Ransomware	**Akira ransomware was first observed in the wild in March 2023** and has since emerged as one of the most active and widely deployed ransomware families across the global threat landscape. Operating under a Ransomware-as-a-Service (RaaS) model, the group consistently leverages double-extortion tactics, demanding payment both for file decryption and to prevent the public release of sensitive data exfiltrated during intrusions. Akira targets organizations across a broad range of sectors, including Manufacturing, Education, and Healthcare, with activity observed across North America, Latin America, Europe, and the Asia-Pacific region. Notably, North America has been a significant hotspot for Akira operations, with a disproportionate share of observed compromises occurring within US-based organizations.	**Initial Access** Targets remote access services such as RDP and VPN through vulnerability exploitation or stolen credentials. **Reconnaissance** Uses network scanning tools like SoftPerfect and Advanced IP Scanner to map the environment and identify targets. **Lateral Movement** Moves laterally using legitimate administrative tools, typically via RDP. **Persistence** Employs techniques such as Kerberoasting and pass-the-hash, and tools like Mimikatz to extract credentials. Known to create new domain accounts to maintain access. **Command and Control** Utilizes remote access tools including AnyDesk, RustDesk, Ngrok, and Cloudflare Tunnel. **Exfiltration** Uses tools such as FileZilla, WinRAR, WinSCP, and Rclone. Data is exfiltrated via protocols like FTP and SFTP, or through cloud storage services such as Mega.



INSIGHTS & OUTLOOK

Threat actors are increasingly bypassing technical controls by targeting humans, enabling rapid escalation from initial access to ransomware deployment or data-leak extortion, significantly reducing defender response time.

The ransomware ecosystem will become even more specialized, with greater collaboration among access brokers, lateral movement operators, and extortion groups. This division of labor will enable faster and more efficient attacks and increase the scale and frequency of high-impact intrusions across organizations of all sizes. Manufacturing and other operational technology-adjacent industries will remain high-risk targets.

With Manufacturing already representing 29% of recorded ransomware incidents in the Americas region in 2025, adversaries are expected to continue prioritizing sectors where downtime has immediate financial and supply chain impacts.

29%

REGIONAL ANALYSIS METHODOLOGY:

It is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the geographic distribution of Darktrace's customer base. For example, within the AMS region, the US represents the largest share of Darktrace customers, meaning insights in this section may be weighted more heavily toward US-based activity.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com