DARKTRACE

Annual Threat Report 2026

cloud attacks

email attacks

vulnerabilities

critical infrastructure

identity

ransomware

Disclaimer

This report is for informational purposes only. While every effort has been made to ensure the accuracy and completeness of the findings, the conclusions are based on the available data at the time, which may be subject to change.

The information does not constitute legal, financial, or professional advice, and readers should consult relevant experts for specific guidance. The views expressed in this report are those of the authors and do not necessarily reflect the views of any specific organization or governmental entity. The report does not guarantee the security of any systems, and ongoing vigilance and adaptive strategies are required to address emerging threats.

This report is provided "as is," without warranties or representations, express or implied, regarding the accuracy or completeness of this report, and **Darktrace will not be liable for any damages or losses arising from the use or reliance on the content.**

Contents

03	**Introduction**	24	Cloud Trends & Analysis
04	**Part 1: The Global Threat Outlook**	26	Ransomware Trends & Analysis
05	The Americas (AMS)	33	Darktrace SOC Trends & Analysis
07	Latin America	35	Campaign Activity Overview
09	Europe	37	**Part 3: Anomaly Detection in Action**
13	Africa	38	**Part 4: Threat Actor Spotlights**
15	Asia-Pacific and Japan (APJ)	38	Understanding Salt Typhoon
18	Critical National Infrastructure Outlook	39	Understanding Scattered Spider
21	**Part 2: Attack Vectors and Evolving TTPs**	40	**Part 5: Outlook for 2026**
21	Email Trends and Analysis	41	**Part 6: Appendices**

Introduction

The Darktrace Annual Threat Report 2026 provides our comprehensive view of the global threat landscape from the past year, and the trends shaping cyber risk in the year ahead. It is intended to provide strategic insight and actionable intelligence for security leaders and practitioners, combining strategic analysis with technical depth.

At Darktrace, we are rooted in the belief that identifying anomalies is crucial to gaining context in each singular environment and across our customer base. Our approach remains distinct: we prioritize these anomalies for behavioral analysis as the cornerstone of detecting both established and emerging threats.

For defenders, the imperative is clear: resilience through automation, behavioral-led detection, and identity-centric security. While the skills gap persists, organizations that embrace adaptive technologies and collaborative intelligence sharing will be best positioned to counter reoccurring waves of intrusions.

This report is the result of extensive analysis conducted across Darktrace's global customer base. Our findings draw on data points collected throughout 2025, including behavioral anomalies, threat notifications, and real-world case studies. We combine these insights through collaboration with national agencies and cyber intelligence vendors, alongside open-source, industry-leading sources such as CERT advisories, and dark web collection, to ensure a comprehensive and accurate view of the threat landscape. Following publication of this report, we will release a series of in-depth, region-specific reports with tailored intelligence and contextual analysis for defenders operating in each region.

We would like to acknowledge the contributions of our global analyst team, incident management team, and development team who worked collaboratively to produce this report. Their expertise ensures that the insights presented here are both actionable and relevant for organizations seeking to strengthen their cyber resilience.

Alexandra Sentenac, Anna Gilbertson, Arnaud Manlius, Calum Hall, Daniel Levy, Emily Megan Lim, Emma Foulger, Eugene Chua, Harriet Rayner, Joanna Ng, Justin Torres, Jung Eun Park, Keanna Grelicha, Logan Murphey, Matthew John, Nahisha Nobregas, Nathan Ly, Nathaniel Bill, Nathaniel Jones, Nicole Wong, Parvatha Ananthakannan, Paul Jennings, Priya Thapa, Rush Rushanth, Ryan Traill, Samantha Gonzalez, Shawn Puckett, Stefan Rowe, Tara Gould, and Tyler Rhea.

Key Takeaways:

The cyber threat environment in 2025 was defined by acceleration, convergence, and complexity.

Adversaries are no longer relying solely on traditional exploits; they are weaponizing artificial intelligence to automate attacks, evade detection, and scale operations at unprecedented speed. This evolution marks a shift from opportunistic campaigns to highly adaptive, intelligence-driven intrusions.

01 Identity is the new perimeter. Identity compromise and trust exploitation have emerged as dominant attack vectors, eclipsing pure vulnerability exploitation. It's easier than ever for attackers to log-in, live off the land, and stay quiet until ready.

02 Cloud and SaaS are systemic risk multipliers. Threat actors are increasingly abusing legitimate services, cloud platforms, and collaboration tools to bypass perimeter controls and embed themselves within trusted ecosystems. Supply chain risk remains acute, with attackers leveraging third-party dependencies and virtual private network (VPN) infrastructure to gain footholds across global networks.

03 Email Remains the Single Most Reliable Attack Channel. Phishing volume, sophistication, and success continue to rise—driven by QR codes, AI-generated content, brand impersonation, and native platform abuse that bypasses legacy filtering.

04 Critical Infrastructure is a Strategic Target. Nation-state operations continue to blur the lines between espionage and disruption, with attribution becoming more complex due to false-flag tactics and infrastructure masking. Telecommunications, Energy, Healthcare, and Transportation are being actively pre-positioned by state-aligned actors for future leverage, disruption, or intelligence collection.

05 Vulnerability management is being outpaced by exploitation speed. Common Vulnerabilities and Exposures (CVE) volumes continue to grow approximately 20% year on year, and exploitation is happening faster than ever – often before disclosure.

Part 01

The Global Threat Outlook

The global cyber threat landscape in 2025 is increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives.

While identity abuse and ransomware remain universal issues, the way cyber threats manifest varies markedly across regions. In 2025, identity compromise emerged as the single most consistent threat across the global threat landscape.

In the United States, the threat environment is dominated by identity-led intrusions and ransomware ecosystems. Software-as-a-Service (SaaS) and Microsoft 365 compromises are the primary initial access vector, often rapidly cascading into double or triple extortion campaigns.

The region's deep SaaS adoption, mature cyber insurance market, and reliance on third-party service providers make it particularly attractive to financially motivated groups seeking high-impact outcomes with short dwell times. Ransomware operations in the US are characterized by specialization and coordination, with access brokers, lateral-movement operators, and extortion groups working in tandem. Nation-state activity, particularly from China-nexus threat actors, continues to illustrate that the US remains the primary target for malicious cyber activity aimed at traditional espionage, intellectual property (IP) theft, and holding critical infrastructure at risk.

Across Latin America, ransomware activity is increasing, but the region also remains disproportionately impacted by credential theft, malware propagation, and data-leak extortion without encryption. Economic volatility, uneven security maturity, and rapid digitization have created conditions where financially motivated actors can achieve returns without the operational risk of full ransomware deployment. At the same time, the region continues to experience nation-aligned cyber activity, particularly against Government, Telecommunications, and Energy, reflecting broader geopolitical and economic engagement.

In Europe, the Middle East and Africa (EMEA), the threat picture is fragmented. Western Europe continues to resemble North America in terms of identity abuse and SaaS intrusion patterns, while parts of Eastern Europe, the Middle East, and Africa experience higher rates of network-based compromise, exposed infrastructure exploitation, and ransomware targeting essential services.

Critical infrastructure and Operational Technology (OT)-adjacent sectors remain a priority across the region, where political instability, regulatory divergence, and legacy systems influence attacker opportunity.

Europe's cyber threat landscape illustrates that cloud-first adoption has reshaped the attack surface, with cloud account and email compromises now surpassing traditional network intrusions, driven by persistent identity security challenges and limited visibility across shared-responsibility environments.

Manufacturing, Financial Services, Technology, and other critical sectors have borne the brunt of this activity, underscoring how cyber risk in Europe has become inseparable from business and national security.

The Middle East have ambitious transformation agendas—such as smart cities, digital government, and large-scale energy and infrastructure modernization—which have expanded the region's attack surface, making critical sectors like Energy, Finance, Telecommunications, Transportation, and Government prime targets. The Africa region is seeing disproportionate growth in network-borne and ransomware-linked attacks, often exploiting exposed VPNs, firewalls, and legacy systems, with the Financial sector firmly atop the list of targeted sectors.

In the Asia-Pacific and Japan region (APJ), threat activity reflects a convergence of state-aligned espionage, financially motivated cybercrime, and opportunistic exploitation of cloud and Internet of Things (IoT) environments. Geopolitical tensions drive sustained Advanced Persistent Threat (APT) activity against Government, Defense, and Telecommunications, while rapid cloud adoption and uneven regulatory enforcement expand the attack surface for ransomware and email-borne threats.

These regional differences underscore a central reality: cyber risk is increasingly contextual. Organizations must understand not only global trends, but the regional threat dynamics that are most likely to shape attacker behaviors within their operating environments. Darktrace plans to expand on these findings with additional regional and sectoral reporting to be released later this year.

■ Regional Outlook:

The Americas (AMS)

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

SaaS/M365 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.

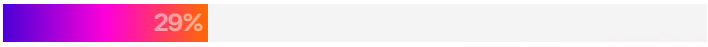
While phishing remains a primary entry point, the impact phase is shifting sharply toward ransomware and data extortion. Ransomware incidents often followed earlier cases of credential compromise or VPN/edge exploitation. Ransomware cases increasingly include pre-encryption data exfiltration, indicating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

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 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.

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.

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 i**ncidents in the Americas region in 2025, adversaries are expected to continue prioritizing sectors where downtime has immediate financial and supply chain impacts.

■ Regional Outlook:

Latin America

Latin America is witnessing a rapid shift from traditional ransomware to data-leak extortion and information stealing malware, focusing on credential theft and sensitive data exfiltration by financially motivated threat actors. Regulatory momentum is building as Brazil, Chile, Argentina, Mexico, and others have enacted data protection laws [1, 2] along with continuous narratives to boost investment in cybersecurity solutions, where 2025 market estimates of USD 18-23 billion are projected to reach USD 30-50 billion by 2030 [3, 4].

However, persistent skills shortages, uneven maturity across national cybersecurity strategies, and reliance on Managed Security Service Providers (MSSPs) continue to challenge regional cyber readiness. Further, these challenges are being amplified by geopolitical dynamics, with China's growing digital footprint through telecommunications and infrastructure projects raising concerns over strategic dependency and surveillance.

Meanwhile, the recent US cyber operation against Venezuela underscores how state-level cyber actions could reshape regional threat perceptions and policy priorities.

Regional Trends and Statistics

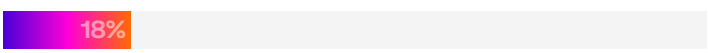
TOP ATTACK VECTORS

Phishing and the use of compromised credentials remain the leading attack vectors. **In 44% of cases** within the region, malware (excluding ransomware) spread following device compromise through these methods.

While phishing dominates, new ransomware strains surged in the region with attribution to BlackSuit, Sauron, Medusa, and Dire Wolf. These cases also signal a shift from data encryption to data leak extortion.

MOST IMPACTED SECTORS

Education was the most impacted sector, making up 18% of all incidents, followed by Public Administration, and Information and Communication.



The Manufacturing and Wholesale/Retail Trade sectors have experienced an increase in cases from the first half of the year to the second, with an increase in incidents of malware propagation, likely driven by accelerated digitization and greater exposure of sensitive data.

MOST IMPACTED COUNTRY

Colombia was consistently the most impacted country in Latin America, followed by Ecuador, Chile, and Mexico. Threats like malware propagation from eCrime and nation-state aligned cyber espionage groups will likely continue to surge in Colombia due to its large economy, high levels of digitalization, and uneven maturity in cybersecurity skills.

REGIONAL VS. GLOBAL COMPARISON

Due to rapid digitalization mixed with uneven security, underinvestment mixed with lagging legislation, and political/economic instability mixed with limited resources, threat actors very likely view Latin America as a profitable region for financially-motivated crimes like ransomware, data-theft, and nation-state espionage.

China's Influence in Latin America

China-nexus activity in Latin America reflects a consistent playbook: rapid exploitation of internet-facing appliances to gain stealthy footholds, followed by long-dwell, tooling-efficient operations. Campaigns leveraging Barracuda ESG (CVE-2023-2868) and Palo Alto PAN-OS (CVE-2024-3400) map to documented People's Republic of China (PRC) tradecraft that prioritizes edge devices for access, collection, and persistence with minimal endpoint noise. Targeting patterns concentrate on Financial institutions in Panama and Colombia, Brazilian Telecommunications, and Colombian Government entities, aligning with strategic intelligence priorities.

Darktrace observed post-access activity anchored by ShadowPad, with DNS-based C2 tunneling, dynamic-link library (DLL) sideloading (e.g., mscorsvc.dll), and LOLBins (WMI/SVCCTL/PsExec) to blend into enterprise operations.

Operators routinely leverage cloud and ORB infrastructure, including Vultr and Cloudflare ArgoTunnel, and deploy Remote Monitoring and Management (RMM) tools (AnyDesk, RustDesk) for resilient commands and lateral movement. Command-line fetch tools (curl/wget) and occasional FTP exfiltration round out a tradecraft set optimized for portability, speed, and operational security.

Looking across these intrusions, the targeting patterns reinforce a broader strategic arc tied to China's expanding economic and digital footprint in Latin America. The focus on financial development organizations, government ministries, telecommunications, and energy mirrors the sectors most intertwined with Beijing's Belt and Road Initiative (BRI) and its "Digital Silk Road" extensions in the region. These institutions hold regulatory, transactional, and infrastructure data that can shape investment environments, forecast political shifts, and enable strategic leverage across BRI-participating economies.

As China moves toward its 2030 objectives, securing supply chains, expanding influence over regional infrastructure, and deepening technological dependencies, cyber operations of this nature provide strategic advantage. The tradecraft observed in Latin America suggests a long-term posture: gaining durable access now to environments that will become increasingly consequential as China's economic and geopolitical statecraft integration across the hemisphere accelerates.

Notable Threat Actors

ACTOR	MOTIVATION & TARGETS	KEY TACTICS
BlindEagle (APT-C-36	**Blind Eagle** characteristically targets government institutions, financial organizations, and critical infrastructure in Latin America with the goal of data exfiltration.	**Initial Access** - T1189 – Drive-by Compromise **Initial Access ICS** - T0865 – Spearphishing Attachment **Initial Access ICS** - T0817 - Drive-by Compromise **Resource Development** - T1588.001 – Malware **Lateral Movement ICS** - T0843 – Program Download **Command and Control** - T1568.002 – Domain Generation Algorithms **Exfiltration - T1041** – Exfiltration Over C2 Channel
Water Saci	**Brazil-focused cybercriminal group** that primarily uses self-propagating malware (named SORVEPOTEL) delivered via WhatsApp to target financial institutions and cryptocurrency exchanges.	**Initial Access** – T1566.003 - Spearphishing via Service **Execution** - T1204.002 – User Execution: Malicious File **Execution** - T1059.005 & T1059.001– Command and Scripting Interpreter: Visual Basic; Command and Scripting Interpreter: PowerShell **Persistence** - T1547.001 – Registry Run Keys / Startup Folder **Credential Access** - T1539 – Steal Web Session Cookie **Command and Control** - T1071.001 – Application Layer Protocol: Web Protocols
SambaSpider	**A Brazil-based cybercrime group that is primarily motivated by financial gain.** Their main target is to steal banking credentials and other sensitive data, predominantly from users and organizations in Latin America. The group is linked to the Mispadu banking trojan.	**Initial Access** - T1566.001 – Phishing: Spearphishing Attachment **Execution** - T1204.002 – User Execution: Malicious File **Execution** - T1059.05 – Command and Scripting Interpreter: VBScript **Execution** - T1027 – Obfuscated Files or Information **Defense Evasion** - T1027 – Obfuscated Files or Information **Defense Evasion** - T1070 – Indicator Removal on Host **Persistence** - T1059 – Command and Scripting Interpreter **Credential Access** - T1555.003 – Credentials from Web Browsers

CASE STUDY

In July 2025, Darktrace identified activity consistent with likely Dire Wolf ransomware after observing unusual file renaming patterns and the appearance of ransom notes on a customer's network. Initial access was gained through the use of the remote management tool TeamViewer, after which a malicious actor created an RDP tunnel, likely to facilitate lateral movement across the environment.

Evidence of both data encryption and data exfiltration was detected. The incident was contained and thoroughly investigated, with restoration efforts carried out in collaboration with partner organizations. Details of the activity were later shared publicly across multiple open-source intelligence (OSINT) channels.

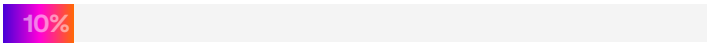
Insights & Outlook

- **Brazil, Mexico, and Colombia have consistently reported the highest number of cases in Latin America** across the Darktrace customer base over the past three years. This trend is likely to continue due to the size of their economies and their geopolitical significance.
- **Top reported threats consist of compromised credentials,** as seen in numerous SaaS intrusion cases, ransomware data-leak extortion, and malware-related cases with increases in informations stealer activity. These threats may continue to be prevalent in the region as financially-motivated threat groups consistently target Latin America.
- **The top attack vector for malware delivery observed by Darktrace is email,** which will likely continue to be a trend in the region as the economy becomes increasingly highly digitized, paired with human vulnerabilities.
- **In 2025, the most impacted sectors in Latin America were the Finance and Public Service-related sectors,** which recorded the highest number of reported cases across multiple countries. However, Latin America may continue to see an increase in attacks against the Technology and Manufacturing sectors, as these sectors encompass critical infrastructure that nation-state threat actors may seek to target.

■ **Regional Outlook:**

Europe

The European cybersecurity market **grew by over 10%** in 2025 [5], reflecting economic and geopolitical factors such as the introduction of mandatory regulation [6] and increased pro-Russian hacktivists targeting organizations in NATO member states and other countries in opposition to Russia's national interests [7].



Regional Trends and Statistics

TOP ATTACK VECTORS

In 2025, cloud account and email compromises accounted for 58% of incidents observed across Darktrace's customer base, significantly exceeding network-based compromises which comprised the remaining 42%.

Attackers are capitalizing on Europe's 'cloud-first' mentality [8] and the corresponding shift of sensitive data to those environments, ongoing challenges securing cloud identities [9] and lack of visibility and control within shared ownership models [10].

MOST IMPACTED SECTORS

Across Europe, the highest share of observed incidents across the Darktrace fleet originated from organizations based in:

- Manufacturing
- Professional scientific and technical activities
- Information and communication
- Financial and insurance
- Construction
- Human health and social work activities

The uptick in attacks on these sectors reflect attackers' shifting focus to the technology stack and infrastructure that underpins operational processes, critical societal functions and permits downstream access to multiple nodes along the supply chain from one source [11].

Notable Threat Actors

ACTOR	MOTIVATION & TARGETS	KEY TACTICS
ShadowPad-linked Chinese state-sponsored actors	**Stealthy persistence;** Manufacturing & critical IT assets	**DNS tunneling** (T1071.004) **SSL C2** (T1071.001) **Privileged credential misuse** (T1078)
Lazarus Group	Democratic People's Republic of Korea (DPRK) state-sponsored APT known for its dual focus on cyber espionage and financial theft.	Social engineering via **fake recruitment campaigns** Use of **trojanized applications** and npm packages **Credential theft** and cryptocurrency wallet targeting **Deployment of remote access tools** (e.g., AnyDesk) and command-and-control via Telegram LOTL techniques using PowerShell and legitimate binaries
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 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.	**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.

Country & Sector Spotlights

The following section presents an analysis of country- and sector-specific attacks observed by Darktrace in Europe in 2025, focusing on key sectors across each country: Financial Services in the UK, Manufacturing in Germany, and Retail in France.

United Kingdom

The UK threat landscape in 2025 was shaped by challenges from both foreign actors and native-English-speaking attackers who targeted key supply chain functions and Technology organizations. The activities of Scattered Spider, a threat group with US and UK affiliates, highlighted the UK's exposure to native-English social engineering and underscored critical supply chain vulnerabilities, most notably in the Jaguar Land Rover attack, which reduced UK gross domestic product (GDP) by 0.1% [12]. Page 38 of this report presents a threat actor profile for Scattered Spider.

In 2025, the UK published its Modern Industrial Strategy, in which the Financial Services sector was listed as a key sector to build investment and deliver a competitive regulatory environment that harnesses the UK's global leadership in Fintech [13]. The UK Financial Services market is becoming increasingly targeted by threat actors interested in this sector, such as Democratic People's Republic of Korea (DPRK)-affiliated actors, particularly in response to heightened US scrutiny in 2025.

CASE STUDY

In 2025, Darktrace detected the activities of Lazarus Group in a UK Forex firm and a UK cryptocurrency organization.

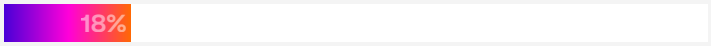
Forex Organization: A developer was socially engineered on a third-party social media platform into running malicious code hosted on GitHub, which likely contained malicious npm packages. From there, the Lazarus group accessed the internal network using Astrill VPN, a third-party VPN commonly associated with the group. Subsequent activity indicated the presence of an infostealer, used for further data collection and exfiltration.

Cryptocurrency organization: Multiple users, including VIPs, were targeted over an extended period by likely Lazarus Group threat actors. In one case, mirroring elements of the group's "Contagious Interview" campaign, a user was approached with a fraudulent job opportunity and instructed to run Terminal commands framed as troubleshooting steps, ultimately installing malicious drivers. Following infection, the compromised devices executed obfuscated Python scripts designed to retrieve additional payloads from Pastebin, scan for crypto-related information, and download further malware such as the Tsunami Injector for keylogging and credential theft. The malware then exfiltrated collected data to a command-and-control server.

Darktrace's Threat Research team also observed the malware removing itself, underscoring the stealthy and operationally disciplined nature of the activity.

France

The Retail sector represents 18% of France's GDP [14]. High-end, luxury fashion in particular holds a strong cultural significance in France, with major international brands and conglomerates operating flagship stores in the Paris region [15]. Thus, these are attractive targets to financially-motivated cybercriminals who hope to capitalize on the data of high net worth individuals for secondary attacks [16].



In 2025, several French luxury brands were targeted by Shiny-Hunters ransomware group. Open-source reporting indicates that the attack likely involved initial access via Salesloft drift and Salesforce account compromise, leading to sensitive customer data exposure [17]. As an example of later stage attacks, Darktrace's Threat Research team detected a Black Friday phishing email campaign attempting to impersonate the luxury fashion brand Louis Vuitton that redirected users to a malicious, newly registered Russian domain. In another attack, the multinational retail giant Auchan experienced a data breach where the data and Personally Identifiable Information (PII) of thousands of customers was stolen from the company's loyalty program and customer information database [18].

While customer PII is a lucrative financial incentive for threat actors, and data-theft attacks on third-party cloud applications like Salesforce have risen this year [19], threat actors with more strategic objectives often leverage unsecured third-party applications as entry points to the wider network. This behavior was exemplified by Darktrace's pre-CVE detection in SAP Netweaver, which was chained with the Auto-Colour backdoor malware.

CASE STUDY

In 2025, Darktrace detected multiple SaaS compromises affecting a French Automobile and Retail distributor. In one case, a VIP was targeted by a phishing attack delivered via Microsoft Forms, enabling the attacker to steal the user's credentials. The attacker then logged in using a third-party commercial VPN and created an email rule that redirected financially-related messages to the Spam folder, likely to obscure signs of fraudulent activity. This activity reflects sustained phishing efforts and classic business email compromise (BEC) tradecraft aimed at concealing financial fraud while maintaining persistence within the victim's SaaS environment.

Germany

Germany hosts Europe's largest industrial economy, **generating 29% of the European Union's (EU) gross value,** and in Manufacturing alone [20]. Rapid digital transformation in German production has placed its Manufacturing industry at the forefront of Industrial Internet of Things (IIoT) adoption [21]. However, such adoption and resultant IT-OT convergence introduce new vulnerabilities to sensitive OT networks.

The presence of IP and patents within this sector make it attractive to both financially-motivated and state-sponsored threat actors [22]. For instance, China's industrial policy places strategic importance on Germany's core sectors, including automotive and mechanical engineering. China's rapid advancements in the automotive industry and its growing share of industrial machinery exports have now surpassed Germany's declining share [23].

Darktrace's analysis of attacks in Germany in 2025 revealed a threat landscape increasingly shaped by SaaS-centric attacks and growing operational complexity. Hybrid email deployments and legacy configurations continue to create visibility gaps, slowing security teams' response times. Attackers are exploiting MFA weaknesses and DNS-based channels at higher rates, blending traditional phishing with more advanced persistence techniques.

CASE STUDY

In 2025, Darktrace detected the activities of state-sponsored malware in a German automation solution manufacturer. ShadowPad is a modular remote access trojan (RAT) that has been deployed by Chinese state-sponsored threat groups [24]. Although the exact initial access vector was unknown, Darktrace's previous analysis of ShadowPad activity in the European Manufacturing sector indicated entry via compromised VPN credentials.

The organization's Domain Controllers (DCs) were beaconing to rare external IPs associated with this malicious backdoor's infrastructure over DNS TXT records, likely using this protocol to tunnel data. Further privilege escalation was observed over external NTLM connections and Kerberos login requests for administrative credentials as the attackers probed internally.

Organizations should continuously monitor privileged accounts and alert on new administrative credential usage on servers. External VPN logins to DCs should be treated as high-severity precursors and paired with MFA hardening and device baselines.

Government & Regulatory Overview

Significant reforms to security policy and regulation advanced across Europe in 2025:

- **The European Union's Digital Operational Resilience Act (DORA)** came into force on January 16, 2023, with mandatory compliance required by January 17, 2025. This is aimed at enhancing the operational resilience of financial institutions and emphasizes proactive measures over reactive financial compensation.
- **The NIS2 Directive** was implemented in several European member states [25]. This widened the list of sectors defined as "important," placing additional "duty of care" requirements that each organization must follow. This includes both proactive and preventative security measures and improved response and reporting following an active threat. Under NIS2, Manufacturing and larger Retail organizations with an annual turnover of over EUR 10 million, among others, are within scope [26, 27]. While NIS2 will help businesses and services build resiliency, implementation may perpetuate existing resource constraints around budget and security expertise [28].
- **The UK government's new Cyber Security and Resilience Bill** was introduced to modernize UK cyber laws, to recognize the risk posed by the supply chain and place industry best-practice, such as the UK National Cyber Security Centre's (NCSC) Cyber Assessment Framework, on firmer footing. Under this, Managed Service Providers and data centers are intended to be added to the scope of regulation to better recognize the increasing reliance on digital services and the vulnerabilities posed by supply chains. This sets clearer government expectations on technical standards and methods organizations will need to follow to prove their resilience [29], shifting the focus from compliance to resilience [30].

Insights & Outlook

- **For Europe,** 2026 presents a continuously evolving cyber landscape shaped by economic growth and technological innovation to ensuring Europe's competitive advantage and resilience amidst heightened geopolitical concerns.
- **Across Europe,** escalating geopolitical threats have highlighted the risks of dependence on US and Chinese providers of cloud, Telecommunications and AI infrastructure. Global competition to achieve 6G technology has placed concerns around the role of Chinese vendors in European infrastructure and their risk [31]. As the EU pushes for physically and logically separate infrastructure [32, 33], organizations should continue to adopt a "trust-but-verify" model, where less trusted areas of the supply chain are continuously assessed and mitigated with risk-based controls.
- **In the UK,** the Government's National Payments Vision and plans to create scalable digital verification and identity calls for more partnerships between the public and private sectors and presents challenges associated with blending variations of centralized and decentralized verification and secure information sharing amongst customers and institutions [34]. Lessons learned from enterprises around securing Identity will be a crucial factor to this.
- **Taken together,** cyber resilience for Europe has become a critical enabler for economic competitiveness, technological leadership and geopolitical stability. Europe's external dependence on governed cloud, Telecommunications, and AI infrastructure has elevated supply chain security from an operational concern to a strategic risk, driving policy shifts toward infrastructure separation, sovereignty, and assurance by design. Successfully delivering these ambitions will depend on sustained public-private collaboration, interoperable design, and the application of enterprise-grade identity security practices at national scale.

Ultimately, Europe's ability to navigate this evolving cyber landscape will be defined by how effectively it balances openness with resilience—leveraging innovation while systematically managing geopolitical and supply-chain risk to preserve trust in its digital future.

■ **Regional Outlook:**

Africa

Africa's digital ecosystem is growing rapidly, but cyber threats are rising just as quickly, with network-based attacks accounting for 76% of compromises detected and ransomware increasing 60% year-over-year, likely due to RaaS operations [35].

70%

Phishing remains the leading entry point at 43%, while the **Finance (27%)** and **Energy (10%)** sectors are the most targeted. **Data exfiltration is also on the rise, observed in 25% of the cases Darktrace detected in the region.**

25% 43%

Connectivity fragility, including recent subsea cable outages, further increases the impact of attacks during disruptions [35]. **Cybercrime now accounts for over 30% of reported crime** in some regions, with scam activity rising by as much as 3,000% in certain Afrian countries and causing significant economic losses, including USD 500m in Nigeria in 2022 and USD 83m in in 2023 [35, 36].

30%

Many nations still lack fully operational Computer Security Incident Response Teams (CSIRTs), though initiatives such as ITU-INTERPOL cyberdrills aim to strengthen response capabilities [37], while generative AI is accelerating threat sophistication through automated and highly tailored phishing and reconnaissance.

Regional Trends and Statistics

76% of compromises seen among Darktrace customers in Africa were network-based. 50% of those network-based attacks were ransomware-related, with around 60% year-on-year growth in ransomware between June 2024 and June 2025 compared with the same period in each of the prior three years.

76%

Ransomware-related activity accounted for 39% of all incidents observed by Darktrace in Africa, with BlackCat (ALPHV) and RansomHub being the most active ransomware groups in the region.

39%

Finance and Energy were the most affected sectors, making up 27% and 10% of incidents respectively, while repeated targeting of Manufacturing and Education was also observed.

10% 27%

Notable Threat Actors

ACTOR	MOTIVATION & TARGETS	KEY TACTICS
BlackCat (Russian RaaS)	Financially motivated; RaaS that targets large enterprises across sectors such as Healthcare, Manufacturing, and critical infrastructure.	**Defense Evasion** (TA0005) **Lateral Movement** (TA0008)
RansomHub (Russian RaaS)	Financially motivated; RaaS that largely targets US-based organizations within the Manufacturing and Healthcare sectors.	**Initial Access** (TA0001), **Execution** (TA0002 **Defense Evasion** (TA0005) **Credential Access** (TA0006) **Impact** (TA0040)

CASE STUDY: Vo1d botnet

First seen in September 2024 by Darktrace [38], Vo1d began as a backdoor for sideloading apps on smart TVs and low-cost Android TV boxes, and later evolved into a multi-function threat for payload deployment, proxy services, and advertisement fraud. It uses XXTEA/RSA encryption [39] and a Domain Generation Algorithm (DGA) to sustain C2 servers even after takedowns [38].

Whilst the botnet is global, spread across more than 200 countries and sustaining over 800,000 IPs daily [40], South Africa was heavily impacted in particular, with Darktrace detecting a high level of activity linked to Vo1d among South African customers.

South Africa ranks among the hardest-hit regions, hosting 8.3% of affected IPs [41] and recording a **13.6% infection rate** in early 2025. Victims spanned critical sectors such as Energy, Retail, Manufacturing, and Public Administration, highlighting the broad impact of this campaign.

External researchers believe infections stem from uncertified Android TV devices often sold on popular marketplaces or malicious apps disguised as legitimate tools. Google confirmed that affected devices were not Play Protect certified [42, 43], meaning they lacked security and compatibility checks.

This case highlights the importance of using certified hardware and software, enforcing regular patching, and taking measures to prevent exploitation of outdated or uncertified technology in critical environments. Additional steps such as network segmentation and egress controls (block unused high ports, monitoring DNS traffic for DGAs) and device controls such as, app allow listing/disabling sideloading, and isolation.

CASE STUDY: React2Shell

Darktrace observed multiple organizations across the African region affected by attackers exploiting CVE-2025-55812, known as React2Shell.

This vulnerability in React server components enables an unauthenticated attacker to achieve remote code execution with a single request. Africa accounted for approximately one-third of all React2Shell-related activity detected globally by Darktrace, with impacted customers located in countries including Kenya and South Africa.

Government & Regulatory Overview

Africa's governments are advancing cybersecurity and data protection while preparing for AI regulation. **South Africa** enforces the Protection of Personal Information Act of 2013 (POPIA), which governs data privacy and breach notifications, and the Cybercrimes Act of 2020, and also introduced the National AI Policy Framework in 2024, expected to be implemented in stages over the next few years.

Kenya combines the Computer Misuse & Cybercrimes Act of 2018 and Data Protection Act of 2019 with its National Cybersecurity Strategy (2022–2027), and plans revisions to address AI misuse and critical infrastructure risks. **Nigeria** mandates breach reporting under the Cybercrimes Act and strengthened privacy through the Data Protection Act (2023), with new sector-specific cybersecurity rules in development. **Mauritius** leads with GDPR-aligned data laws and the Cybersecurity & Cybercrime Act of 2021, and its proposed Blueprint for Mauritius 2025–2029 strategy plans to update AI and cyber regulations and create an AI Office and a national cyber resilience agency.

Insights & Outlook

Phishing emails remain the leading cause of compromise in Africa, with 67% of SaaS incidents originating from phishing, making up 16% of all initial access vectors observed by Darktrace in the region.

This trend is reinforced globally by the widespread availability of generative AI, which makes writing more convincing phishing emails much faster and more accessible.

VPNs and exposed internet-facing systems are also major attack vectors. One-third of known network-based intrusions involved VPN access, **while 27% stemmed from exploited CVEs and exposed services.**

About 57% of identified ransomware strains were RaaS, representing half of all ransomware cases; the comparatively lower observed RaaS use in Africa may suggest more targeted, goal-driven intrusions rather than purely financial campaigns.

Data exfiltration has also risen over the last three years, potentially reflecting pre-ransomware activity detected earlier in the kill chain.

■ **Regional Outlook:**

Asia-Pacific and Japan (APJ)

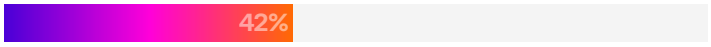
The APJ region is undergoing rapid digital transformation, driven by large-scale adoption of cloud services, 5G connectivity, and AI integration. These advancements, while enabling innovation, introduce significant challenges around data sovereignty, misconfigurations, and legacy system vulnerabilities. Geopolitical tensions, such as the South China Sea dispute, strained DPRK-Republic of Korea (RoK) relations, and global conflicts fuel state-sponsored cyber campaigns and disinformation operations.

Fragmented regulatory frameworks and uneven cybersecurity maturity across economies amplify exposure, leaving critical infrastructure, financial institutions, and government entities particularly vulnerable to ransomware, phishing, and AI-powered attacks.

Regional Trends and Statistics

84% of APJ organizations agree that AI-powered cyber threats are already impacting them and will continue to do so.

Only 42% of APJ organizations have a formal policy for safe AI use, and confidence in traditional solutions has fallen 14 points; 55% now say those tools don't adequately stop AI-powered attacks (up from 41% in 2024).



Phishing targeting pattern: In APJ, **14% of phishing emails** target VIP users significantly lower than the global 25%, indicating broader, organization-wide phishing rather than VIP-heavy campaigns.

Source: Darktrace's APJ Threat Landscape Report

Notable Threat Actors

ACTOR	MOTIVATION & TARGETS	KEY TACTICS
Lazarus Group (DPRK-linked)	Strategic espionage; financial gain targeting RoK government, defense, and cryptocurrency firms	**Spear phishing** (T1566) **Supply-chain exploits** (T1195)
APT40 (China-nexus)	Espionage aligned with BRI; targets Southeast Asian Governments, Telecommunications, Australia, Japan	**Exploit public-facing apps** (T1190) **Spear phishing** (T1566) **Encrypted webshells** (T1505.003)
MirrorFace (Earth Kasha)	Espionage targeting Japanese media, political organizations, research institutions	**Spear phishing** (T1566) **Malware deployment** (T1204.002)
Mustang Panda	Espionage including against Southeast Asian law enforcement agency.	**Spear phishing** (T1566) **Remote Access Tool** (T1219) **Registry persistence** (T1547) **LOTL techniques** (T1059.001)

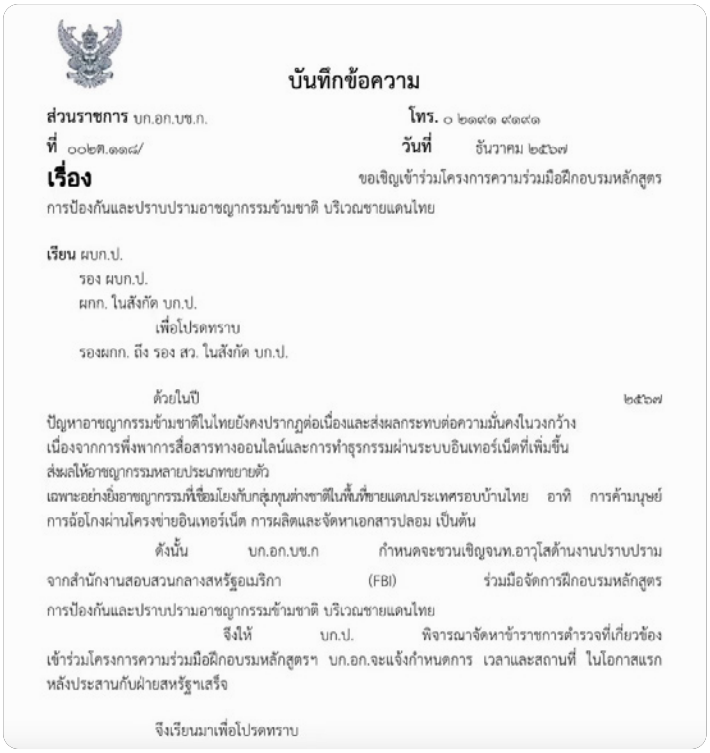
CASE STUDY: Mustang Panda

In February 2025, Darktrace researchers identified a Mustang Panda campaign targeting the Royal Thai Police to deliver the Yokai backdoor. The initial file was a RAR archive named “ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.rar (English: Very urgent, please join the cooperation project to train the FBI course.rar)”.

While the initial access vector is unknown, it was highly likely delivered via phishing email. Inside the archive was an LNK shortcut file, ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.docx.lnk, a disguised PDF file, and a folder named $Recycle.bin.

The shortcut file executes ftp.exe, which then processes the commands embedded in the disguised PDF file as an FTP script, an automated sequence of FTP commands. The installed payload, PrnInstallerNew.exe, is a maliciously altered version of legitimate PDF printer software. It employs detection-evasion techniques by dynamically constructing and invoking system functions at runtime rather than referencing them directly, making its behavior more difficult for security tools to analyze.

After resolving its API calls, the malware connects to its C2 server over port 443, sending the hostname and awaiting further instructions. To maintain persistence, it adds itself to the user’s startup registry, ensuring it executes each time the user logs in.



บันทึกข้อความ

ส่วนราชการ บก.อก.บช.ก. โทร. ๐ ๒๑๔๑ ๙๑๙๑

ที่ ๐๐๒๓.๑๑๔/ วันที่ ธันวาคม ๒๕๖๗

เรื่อง ขอเชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย

เรียน ผบก.ป.
รอง ผบก.ป.
ผกก. ในสังกัด บก.ป.
เพื่อโปรดทราบ
รองผกก. ถึง รอง สว. ในสังกัด บก.ป.

ด้วยในปี ๒๕๖๗ ปัญหาอาชญากรรมข้ามชาติในไทยยังคงปรากฏต่อเนื่องและส่งผลกระทบต่อความมั่นคงในวงกว้าง เนื่องจากการพึ่งพาการสื่อสารทางออนไลน์และการทำธุรกรรมผ่านระบบอินเทอร์เน็ตที่เพิ่มขึ้น ส่งผลให้อาชญากรรมหลายประเภทขยายตัว เฉพาะอย่างยิ่งอาชญากรรมที่เชื่อมโยงกับกลุ่มทุนต่างชาติในพื้นที่ชายแดนประเทศรอบบ้านไทย อาทิ การค้ามนุษย์ การฉ้อโกงผ่านโครงข่ายอินเทอร์เน็ต การผลิตและจัดหาเอกสารปลอม เป็นต้น

ดังนั้น บก.อก.บช.ก กำหนดจะขอเชิญจนท.อาวุโสด้านงานปราบปราม จากสำนักงานสอบสวนกลางสหรัฐอเมริกา (FBI) ร่วมมือจัดการฝึกอบรมหลักสูตร การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย

จึงให้ บก.ป. พิจารณาจัดหาข้าราชการตำรวจที่เกี่ยวข้อง เข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตรฯ บก.อก.จะแจ้งกำหนดการ เวลาและสถานที่ ในโอกาสแรก หลังประสานกับฝ่ายสหรัฐฯเสร็จ

จึงเรียนมาเพื่อโปรดทราบ

Figure 01: Decoy docx file ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.docx. (English: Very urgent, please join the cooperative training project for the FBI course.docx)

CASE STUDY: WAZUH EXPLOIT

In 2025, attackers exploited an unsafe deserialization vulnerability in Wazuh Manager (CVE202524016), enabling remote code execution.

This allowed adversaries to deliver Mirai botnet payloads across IoT devices, leveraging compromised systems for large-scale botnet attacks. The Wazuh exploit enabled Mirai botnet spread across IoT devices, creating risks of operational disruption and supply chain impact. This highlights the need for timely patching of vulnerable platforms, strict network segmentation, and limiting remote access tools. Organizations should also leverage AI-driven detection to spot anomalous activity early and reduce dwell time.

CASE STUDY: GH0STRAT

In May 2025, attackers deployed the remote access trojan Gh0stRAT against a customer in the APJ region. Initial activity involved connections to a suspicious domain, which subsequently triggered repeated executable downloads from a rare IP address associated with the Hong Kong-based hosting provider AS138995 Antbox Networks Limited.

The frequent abuse of hosting providers within the APJ region enables malicious C2 traffic to blend more easily with legitimate network activity common among APJ-based organizations. To counter this, organizations should leverage AI-driven detection capable of identifying anomalous external connections that may represent C2 communication—regardless of geographic location.

Government & Regulatory Overview

Governments across APJ are tightening cybersecurity laws to address rising threats and AI risks:

- Japan's Active Cyber Defense Act will come into effect 2026, enabling preemptive action and mandatory reporting for critical infrastructure, alongside SME-focused awareness programs.
- RoK introduced an overarching Framework Act on AI, enforced in January of 2026, aimed at curbing the misuse of generative AI, and strengthened privacy through the Personal Information Protection Act, most recently amended in 2023, while shifting to a proactive national defense strategy.
- Australia launched the Cybersecurity Act (2024) with ransomware payment reporting and adopted global standards for OT and AI security.
- Across Southeast Asia, Association of Southeast Asian Nations (ASEAN) initiatives like the Cybersecurity Cooperation Strategy and Singapore's planned Digital Infrastructure Act aim to secure cloud ecosystems and critical digital infrastructure.

Insights & Outlook

- Organizations in APJ continue to face persistent vulnerabilities stemming from misconfigurations, phishing, and insider risks.
- AI-driven attacks are on the rise, enabling more sophisticated phishing and accelerating malware development.
- At the same time, hybrid cloud environments and increasing IT-OT integration are expanding the regional attack surface, while fragmented regulations and reliance on legacy systems contribute to systemic weaknesses.
- Looking ahead, the region is likely to see continued growth in AI-powered phishing and identity abuse, along with a rise in attacks targeting critical infrastructure and OT systems. Regulatory attention on AI and cloud security will intensify, though enforcement is expected to remain inconsistent across APJ.

Critical National Infrastructure Outlook

The accelerating convergence of geopolitical tensions and the digital transformation of critical infrastructure has made cybersecurity inseparable from statecraft. Critical National Infrastructure (CNI) has become a strategic battleground—where influence, coercion, and national power increasingly play out in cyberspace [44]. Darktrace observed three recurring trends in analysis of the motivation and objectives behind these attacks:

01 Attacks on CNI to disrupt national services, threatening national security and public stability [45]

The Russian-Ukraine conflict has led to an increase in cyber-physical attacks on Ukrainian and Western energy infrastructure [46] from state-sponsored and criminal hacktivists [47]. The interdependency between CNI sectors exacerbated the impact of these attacks, where disruptions to power supply further hampered healthcare delivery [48]. The Health-ISAC warned EU healthcare organizations to consider chronic energy shortages in their business resilience plans for 2025 [49].

02 Attacks on CNI to further national strategic objectives

Chinese APT activity in 2025 highlights China's changing use of cyber capabilities for passive outcomes, like espionage, to active disruption. Salt Typhoon's infiltration of US telecommunications infrastructure enabled intelligence gathering via access to US government communication for the potential to be used during conflict [50]. While Salt Typhoon's most publicized attacks in 2025 pertained to the US, Darktrace detected this group's exploitation of a Citrix Netscaler vulnerability to gain access to a European Telecommunications organization, demonstrating the group's global strategic objectives.

Volt Typhoon, operated by the People's Liberation Army, deployed implants in several US CNI organizations, including Energy, as pre-positioning for disruptive OT attacks to dissuade US intervention in China's conflict with Taiwan [47, 51].

03 Usage of proxy agents to further geopolitical interests

State-sponsored attacks are sometimes conducted by hybrid groups that are allowed to conduct financially-motivated operations to supplement income and reduce the cost of operations [52]. This is common for DPRK threat actors [53], who target the Financial Services sector and use profits generated for the regime to support their intelligence gathering efforts [52].

In 2025, Darktrace observed DPRK-affiliated threat actors employing multiple intrusion methods to achieve a common objective: cryptocurrency mining. These activities included the deployment of trojanized malware within a UK financial services organization and the exploitation of the React2Shell zero-day vulnerability in a Singapore-based financial services organization.

Sector Trends

Darktrace performed deep-dives into the threat landscape across the financial services, healthcare, telecommunications and energy sectors and observed the following trends in 2025:

01 Attackers exploit trust within CNI

At the individual level: Darktrace observed a resurgence in ClickFix social engineering in 2025, which exploits the trust that users place in seemingly legitimate websites [54]. While browsing for jobs on a popular search engine, a user in a UK hospital accessed a compromised site and was presented with a fake CAPTCHA verification that prompted them to execute PowerShell commands, which then downloaded additional scripts and posted data externally.

This tactic is also prevalent within the Financial Services and Energy sectors. Darktrace detected activity attributed to the Kongtuke group using ClickFix social engineering to download MintsLoader during a compromise targeting a water management company in the oil and gas industry.

At the technology level: Darktrace's threat actor profiling of Salt Typhoon and Liminal Panda exemplify how threat actors exploit trust at this level to move laterally across sensitive Telecommunications networks. Techniques such as DLL sideloading (Salt Typhoon) and the exploitation of eDNS servers (Liminal Panda), which are trusted across different mobile operators, take advantage of legitimate technologies that often have privileged access.

At the system level: Attackers exploit interconnections within sectors, such as Healthcare. For example, in 2025, INC Ransomware, a RaaS group, used RDP to exploit the Citrix gateway shared between two hospitals in Europe to gain initial access. This exemplifies the importance of monitoring even the "trusted perimeter" between organizations.

02 Ransomware and phishing attacks on CNI leverage data exfiltration for financial gain

Darktrace detected RaaS actors such as INC Ransom and TridentLocker prioritizing data exfiltration for extortion in attacks targeting hospitals and energy producers. In some attacks, encryption was not required for the attacker to achieve their objectives. Data exfiltration was performed using legitimate cloud file transfer software such as Mega, OneDrive and GoFile, or native protocols such as FTP, which would often bypass signature-based detections.

03 A Critical identity crisis across IT and OT

In 2025, a significant proportion of attacks detected in CNI organizations targeted identity, even in sectors with major OT infrastructure. As outlined in the sector-focused reports published by Darktrace in 2025, data from Darktrace / EMAIL indicates that VIP-targeted phishing accounts for 33% of phishing emails in the Healthcare sector, 20% in the Energy sector, and 30% in the Finance sector.

In the Telecommunications sector, Darktrace detected medium-confidence indicators of Liminal Panda targeting the SaaS accounts of senior engineers from a European organization involved in defense. This specific targeting of individuals with access to confidential information reflects the group's overall tradecraft, using their research and development capabilities to target vendor-specific infrastructure.

Automation is also used to scale these attacks. Darktrace observed the use of Axios to bypass user MFA by collecting tokens and maintaining long-term persistence to the SaaS account within an Energy producer, where the attacker took a "lay-and-wait" approach, with no other impact observed for several months. This HTTP client library was previously only observed in campaigns targeting executives and managers in the finance, healthcare and manufacturing sectors, but has since been observed automating compromises on "everyday users" in other sectors [55].

The adoption of cloud services within the workforce has also introduced new attack vectors. As discussed in Darktrace's 2025 Energy sector report, Darktrace researchers uncovered a Stage 1 Industrial Control System (ICS) attack originating from a compromised SaaS account within a European renewable energy organization. In this incident, the attacker used PerfectData Software to exfiltrate mail data before downloading numerous Mahlo PLC configuration files stored in the cloud.

In the Telecommunications sector, Darktrace identified a compromise of a US router supplier's Salesforce account via the Salesloft Drift supply chain attack. The access was then used to download Salesforce data, potentially granting the attacker downstream access to other organizations. This attack vector exemplifies how traditional challenges securing identity also threatens cloud security, where threats associated with privilege creep and the lack of visibility across different identities and are amplified across a fragmented ecosystem of multiple cloud providers and SaaS applications.

In sectors where identity-driven attacks are more common, such as Healthcare, Darktrace observed the use of sophisticated phishing emails to enable lateral proliferation. The incident began with browser hijacking that compromised a senior IT support staff member at a Healthcare administration organization. From there, operationally accurate phishing emails were sent from the compromised account, which held trusted access to other users and organizations.

The prevalence of identity compromises in CNI sectors signals the shift from malware-driven compromise but also deliberate targeting of supply chain functions.

04 Attackers target CNI via weaker nodes of its supply chain

The impact of major Healthcare supply chain attacks in 2024 continued into the following year. In June 2025, a patient death was linked to the opportunistic ransomware attack on Synnovis, a pathology provider serving a network of UK hospitals [56]. In July 2025, the number of individuals affected by the ransomware attack on Change Healthcare, a US payment systems supplier, continued to rise [57], underscoring systemic weaknesses across the sector's supply chain.

Generally, supply chain vulnerabilities in widely used third-party applications have become a major vector for initial access and data exfiltration within CNI. In the Finance sector, RaaS actors such as Cl0p have evolved their tactics, shifting from targeting individual victims directly via phishing for initial access in 2019, to widespread reach via zero-day vulnerabilities in enterprise file transfer software, such as Cleo software in 2025 [58].

In 2025, Darktrace observed how Decentralized Finance (DeFi) is expanding this sector's attack surface as fintech organizations integrate with core functions, detecting significant attacks involving DPRK-linked BeaverTail malware deployed via trojan job applications targeting crypto developers in finance [59].

Similarly, Darktrace's research in the Energy sector also noted an increasing target on renewable energy that is not commensurate with these organizations' investment in cyber controls. In a European renewable energy producer, Darktrace detected Mints-Loader malware performing browser credential harvesting, likely in preparation for second stage attacks.

In another instance, a GuLoader malware campaign was observed with targeted phishing activity against Middle Eastern Energy organizations, using oil and gas-themed lures impersonating trusted and well-known suppliers.

Initial access is achieved via malicious Microsoft Excel attachments containing heavily obfuscated macros that stage VBScript and PowerShell payloads, culminating in in-memory shellcode execution and delivery of secondary RATs (e.g., Remcos, NetWire, AgentTesla).

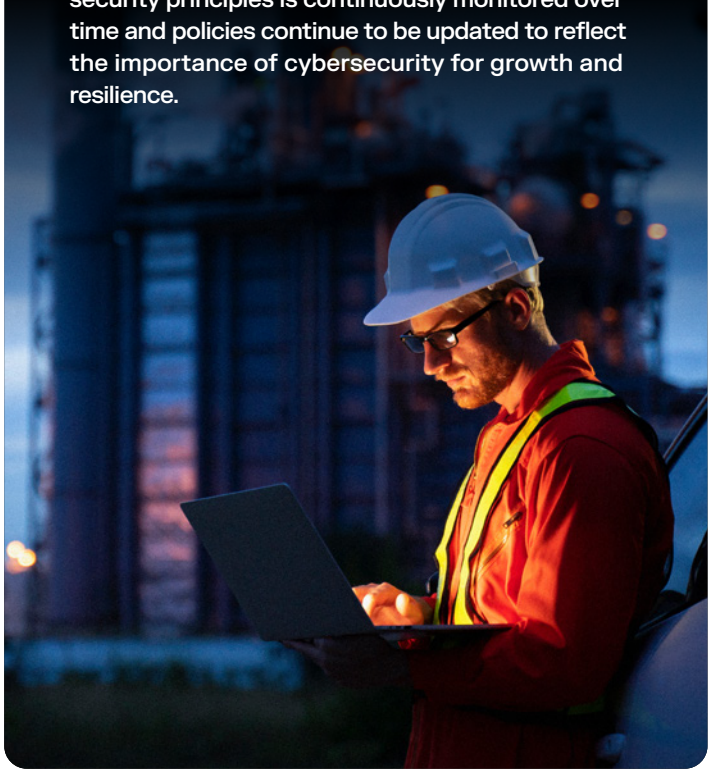
For security leaders, these campaigns underscore persistent, sector-specific targeting and third-party brand abuse, reinforcing the need for strong phishing resilience, macro abuse detection, and visibility into suspicious and persistence behaviors.

Outlook and Recommendations for Defenders and Policymakers

The use of CNI as a strategic battleground by state-sponsored actors is likely to continue, reinforcing the importance of achieving defensive superiority. The usage of legitimate tooling, custom malware and zero-day exploits highlights the need to adopt modern defenses that can continue to evolve with the threat landscape.

The reality of IT and OT convergence and growing attack surface of CNI underscores the importance of resource prioritization in OT and legacy infrastructure [60], Darktrace detected several attacks on CNI that also exploited gaps in basic security controls, including long patch management cycles, internet-facing severs and OT devices, unmonitored edge infrastructure and dormant privileged accounts.

It is important that adherence with these basic security principles is continuously monitored over time and policies continue to be updated to reflect the importance of cybersecurity for growth and resilience.



Part 02

Attack Vectors and Evolving TTPs

Email Trends and Analysis

In 2025, Darktrace / EMAIL™ detected over 32,000,000 high-confidence phishing emails across its global fleet. Analysis of these phishing emails revealed the following key totals:

8.2m Number of **phishing emails sent to VIPs:** Over 8.2 million (representing over 25% percent of all phishing emails detected)

1.6m Total number of phishing emails with **newly created domains:** Over 1.6 million

1.2m Number of **QR code phishing emails:** Over 1.2 million

70% Emails successfully passing **DMARC Authentication**

41% Emails were **spear-phishing attempts**

38% Emails contained **novel social engineering features**

33% Emails containing a **large amount of text** (over 1,000 characters or around 200 words)

By leveraging trusted platforms and domains, malicious actors can bypass security measures and increase the likelihood of their phishing attempts being carried out successfully.

As such, the abuse of senders and legitimate services continues to be a leveraged approach and method for threat actors in 2025.

Regional Insights

Regional Phishing Trends at a Glance

AMERICAS	EMEA	AFRICA	APJ
32% Phishing emails targeting VIPs	**20%** Phishing emails targeting VIPs	**17%** Phishing emails targeting VIPs	**14%** Phishing emails targeting VIPs
5% QR code phishing emails	**3%** QR code phishing emails	**3%** QR code phishing emails	**9%** QR code phishing emails
72% Successfully passed DMARC Authentication	**73%** Successfully passed DMARC Authentication	**80%** Successfully passed DMARC Authentication	**66%** Successfully passed DMARC Authentication
47% Spear-phishing attempts	**39%** Spear-phishing attempts	**37%** Spear-phishing attempts	**35%** Spear-phishing attempts
40% of emails contained novel social engineering features	**38%** of emails contained novel social engineering features	**40%** of emails contained novel social engineering features	**41%** of emails contained novel social engineering features

Focusing on emails from the final six months of 2025, the proportion of phishing emails targeting VIPs was noticeably higher in AMS compared with EMEA and APJ, **reaching 32%** and indicating a trend toward more focused targeting in this region. Meanwhile, the proportion of phishing emails containing QR codes was highest in APJ.

32%

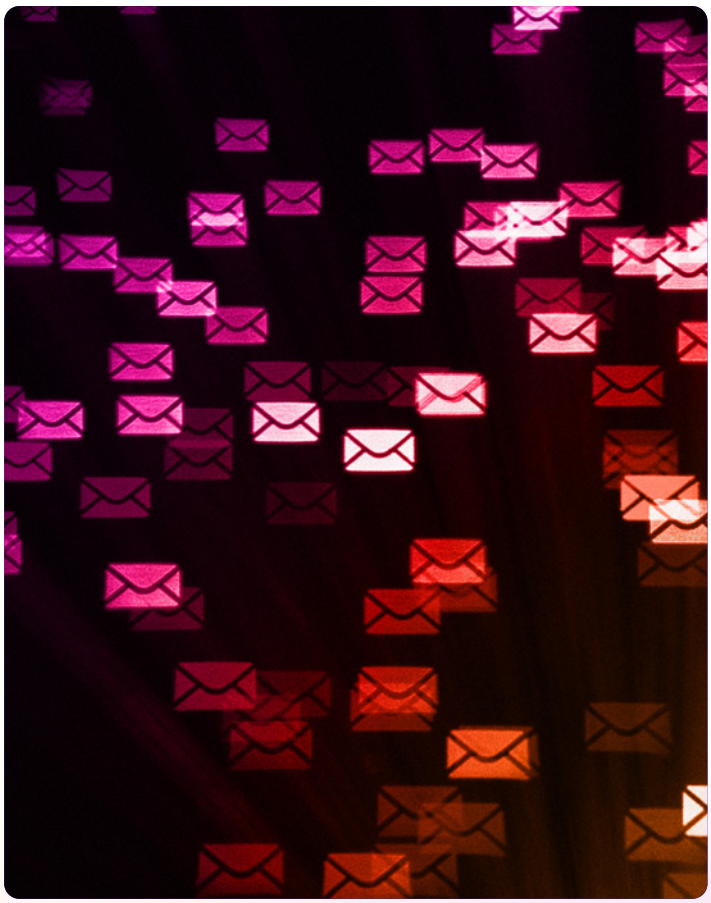
Phishing emails received by Darktrace customers within Africa showed notable differences compared with other regions. Over 40% of phishing emails contained a large amount of text, and 80% successfully passed DMARC authentication.

Taken together, these findings highlight significant regional variation in phishing strategies, suggesting that threat actors are tailoring their approaches to local defensive postures and user behavior patterns.

01 **AMS** shows signs of increasingly targeted, VIP-focused activity;

02 **APJ** demonstrates a preference for QR code-based phishing, aligning with the widespread use of this technology in the region; and

03 **Africa** stands out for the use of longer, text-heavy emails, indicating a deliberate emphasis on social engineering.



Evolving Email Threats

A comparison to 2024

A comparison between 2024 and 2025 of the proportion of phishing emails according to threat type observed by Darktrace.

An increase in malicious QR codes

Darktrace observed over 940,000 phishing emails containing QR codes in 2024 [61] and the number rose to 1.2 million in 2025, with the overall proportion of phishing emails containing QR codes increasing as well over that time period. The overall growth in QR code-phishing is based on its evasion against security filters industry expansion as well as mobile devices becoming a primary target.

Email threats have continued to grow in sophistication, with QR code phishing being a clear example of this in 2025. Multiple new techniques were reported by OSINT sources and observed by Darktrace, including [62], in which a QR code is split into two distinct images, and QR code nesting, where a legitimate QR code is embedded [63]. This escalation in sophistication demonstrates the ongoing race between defenders and attackers as new techniques are developed.

An increasing use of newly created domains

In 2025, Darktrace also observed roughly 1.6 million phishing emails with newly created domains, a proportional increase when compared with 2024. Newly created domains are attractive to threat actors as they offer a reputation with very minimal security history, making them less likely to be blocked by security filtering.

These domains can be quickly registered, customized to visually resemble legitimate brands, and discarded just as fast to evade detection. Since many traditional security tools rely on reputation scoring or age-based heuristics, the short lifespan and rapid turnover of new domains can help attackers stay ahead of defences while delivering malicious links that appear deceptively trustworthy to victims.

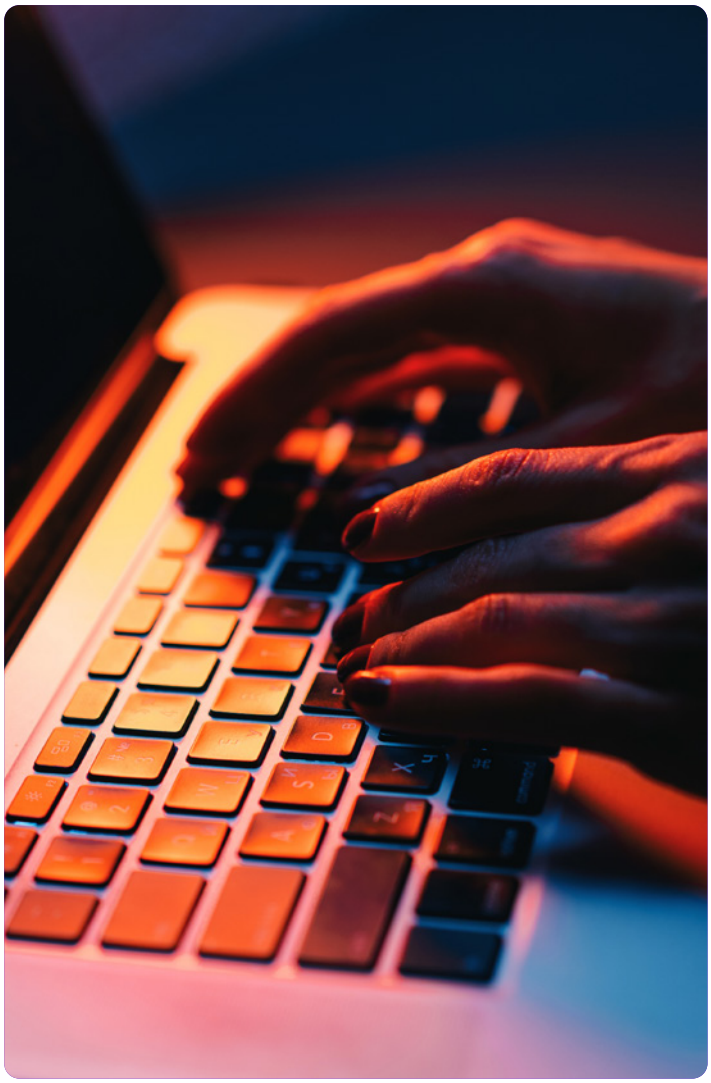
An increasing impact from generative AI

Increases in proportion were also seen for spear-phishing, novel social engineering, and emails containing a large amount of text in 2025 compared with 2024, suggesting further shifts towards targeted email attacks and the possible use of LLMs to generate email text.

An increase in seasonal campaigns & consumer brand abuse

In November and December 2025, phishing totals seen by Darktracenearly doubled what was observed in 2024.

This upward trend is unsurprising, as phishing tends to spike during the holiday season, particularly around retail events like Black Friday and Cyber Monday. Phishing emails were particularly affected in the AMS region during this period, with Darktrace seeing increases in more specific techniques: those involving newly created domains spiked in November within AMS, and phishing emails involving brand impersonation increased by over 40,000 in December in the US alone.



Notably, phishing attacks taking advantage of Black Friday skyrocketed by 620% in the weeks leading up to the holiday weekend in 2025 [64, 65].

Further analysis from October through December 1, 2025, revealed some notable patterns that can be found below:

- **Black Friday-related phishing** skyrocketed in November, surpassing October totals and seeing more than 32,000 malicious emails while being compared to the previous month (roughly a 1,317% increase).
- Attackers are **front-loading phishing campaigns** ahead of peak shopping days to exploit early deals and consumer anticipation, with significant volumes of Black Friday phishing seen in the early weeks of November.
- **Cyber Monday phishing** remains lower in volume, but its growth rate is significant overall.
- **Global consumer brands** continue to be a primary lure, showcasing consistent growth; in November, over 45,000 phishing emails tied to major global consumer vendors were observed.
- Among US consumer vendors, **brand abuse-related phishing** rose by 58% in November from October, demonstrating the risks US vendors face during seasonal campaigns.

Cloud Trends & Analysis

Trends and Statistics

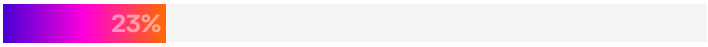
- An estimated **94%** of organizations worldwide are using cloud computing
- **55%** of organizations are multi-cloud as of 2025
- Darktrace data indicates Azure as having **the most activity**

Overview

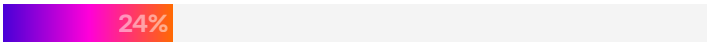
With an estimated 94% of organizations worldwide using cloud computing to run applications, store data or support operations, **cloud security is now a core risk for most enterprises** [85].

The industries adapting to cloud technologies include Technology, Finance, Healthcare, Retail, Government, Energy, Manufacturing and Education. The evolution and adaptation of cloud computing has introduced organizations to increased security risks. These risks include misconfiguration, vulnerabilities, malware, Identity and Access Management (IAM) abuse and supply chain compromise.

Still the top threat to cloud security, misconfigurations account for an estimated 23% of security incidents [86]. Misconfigurations are usually the result of human error, complex setups, or default configurations being used by organizations. Misconfigurations can include publicly accessible storage and databases, leaked credentials, insecure APIs, and misconfigured IAM roles leading to excessive permissions.



Vulnerabilities remain an issue in the cloud with a reported 24% of security incidents resulting from unpatched vulnerabilities [87].



In December 2025, the critical vulnerability CVE-2025-55182, dubbed "React2Shell", was publicly disclosed. The vulnerability is a remote code execution flaw in React Server Components that allows for an unauthenticated attacker to gain remote code execution with a single request. The severity of this vulnerability and ease of exploitability led to Darktrace observing threat actors opportunistically exploiting it within hours of a React honeypot being set up.

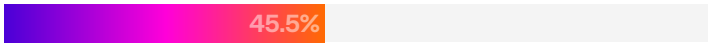
In order to capture real-time attacks, Darktrace operates a global honeypot network, called "Cloudypots," designed to observe malicious activity across a wide array of services, protocols, and cloud platforms. These honeypots provide real-time insights into the techniques, tools, and malware actively targeting Internet-facing infrastructure. The services included in Cloudypots are Docker, Jupyter, Selenium, React, Jenkins, Gitlab and RocketMQ. Darktrace Cloudypots has uncovered multiple novel malware campaigns against these services and provides understanding on how the threat landscape is evolving.

Global Activity Distribution

The data Darktrace has collected over the past year shows that malicious activity originates from a globally diverse set of regions, though not evenly distributed. Based on raw event volume and geo-located by origin IP address, **China accounts for 35.4%** of activity, followed by **South Korea (15.9%),** the **United States (13.5%),** and **Germany (11.4%).** Other countries, including the Netherlands, France, Brazil, Peru, Russia, and Indonesia, contribute smaller shares. Much of this activity aligns with the widespread abuse of cloud infrastructure and compromised endpoints being used as scanning platforms.

Taken together, these observations underscore that while malicious activity is globally distributed, it is not a reliable data point for actor origin or sponsorship. The concentration of activity in certain countries largely reflects the geographic footprint of cloud providers and compromised or abused infrastructure rather than the true location of threat actors or any indication of meaningful attribution.

However, raw event counts are heavily influenced by a small number of hyperactive sources. When the data is normalized so that each unique IP contributes equally, China still leads, with around 45.5% of unique malicious sources, but some regions, such as South Korea, drop dramatically. This shows how much a small number of large-scale campaigns can make up a large portion of overall attacks.



Honeypot Targeting by Service

Honeypot interactions are not evenly distributed across services. Based on total events, Cowrie (SSH and Telnet honeypot) received the largest share at **36.8%,** followed by **Docker at 28.3%, Selenium Grid at 20.4%,** and **Jupyter Notebook at 14.4%.** These trends reflect the services most frequently targeted for unauthorized access, remote execution, or container manipulation.

Once the data is normalized per unique IP, important differences emerge. Selenium and Jupyter, both popular targets for cryptomining-related campaigns, drop sharply from 20.4% to 1.2% and 14.4% to 9.3% respectively, showing how small clusters of hostile infrastructure can generate disproportionate volumes of traffic. Docker, by contrast, becomes the dominant target, rising to 54.3% of unique malicious sources and indicates a broader, more distributed threat landscape that underscores its strategic attractiveness for opportunistic and scalable cryptomining campaigns.

Cloud Service Provider Breakdown

A major component of the honeypot deployment strategy is its distribution across Azure, Google Cloud Platform (GCP), AWS, and Darktrace's own Cloudypots platform.

Across all malware samples collected, Darktrace's Cloudypots honeypot system accounts for 84.1% of them due to its ability to allow full execution of attacker payloads. However, comparing the three major cloud platforms where we host our lower interaction honeypots reveals attacker preferences:

Azure captures 43.5% of other malware samples, with activity spread across the US (17.6%), Asia (15.3%), and Europe (10.6%). This makes Azure the most targeted provider as seen in Darktrace's data.

43.3%

GCP accounts for 33.2%, with a near-even distribution across Asia (12.6%), Europe (12%), and the US (8.6%).

33.2%

AWS contributes 23.2%, with Asia (9.3%), Europe (7.6%), and the US (6.3%) receiving similar levels of activity. AWS activity is lower overall, possibly due to stricter abuse controls or attacker cost-efficiency considerations.

23.2%

Case Studies

JUPYTER NOTEBOOKS TARGETED IN CRYPTOMINING CAMPAIGN

In February 2025, Darktrace researchers identified a cryptomining campaign that targets publicly exposed or misconfigured Jupyter Notebook instances to deploy cryptomining software on both Windows and Linux systems.

AWS INTRUSIONS

Darktrace details two incidents, taking place in February and March 2025, targeting AWS environments. In these cases, threat actors exfiltrated corporate data, and in one instance, were able to detonate ransomware in a customer's environment.

PUMABOT

PumaBot is a novel botnet first identified in May 2025 by Darktrace researchers, written in the Go programming language and designed to target Linux based IoT devices, with a particular focus on surveillance hardware.

SHADOWV2 DDOS

ShadowV2 is a novel botnet discovered by Darktrace researchers in September 2025 that targets docker installations.

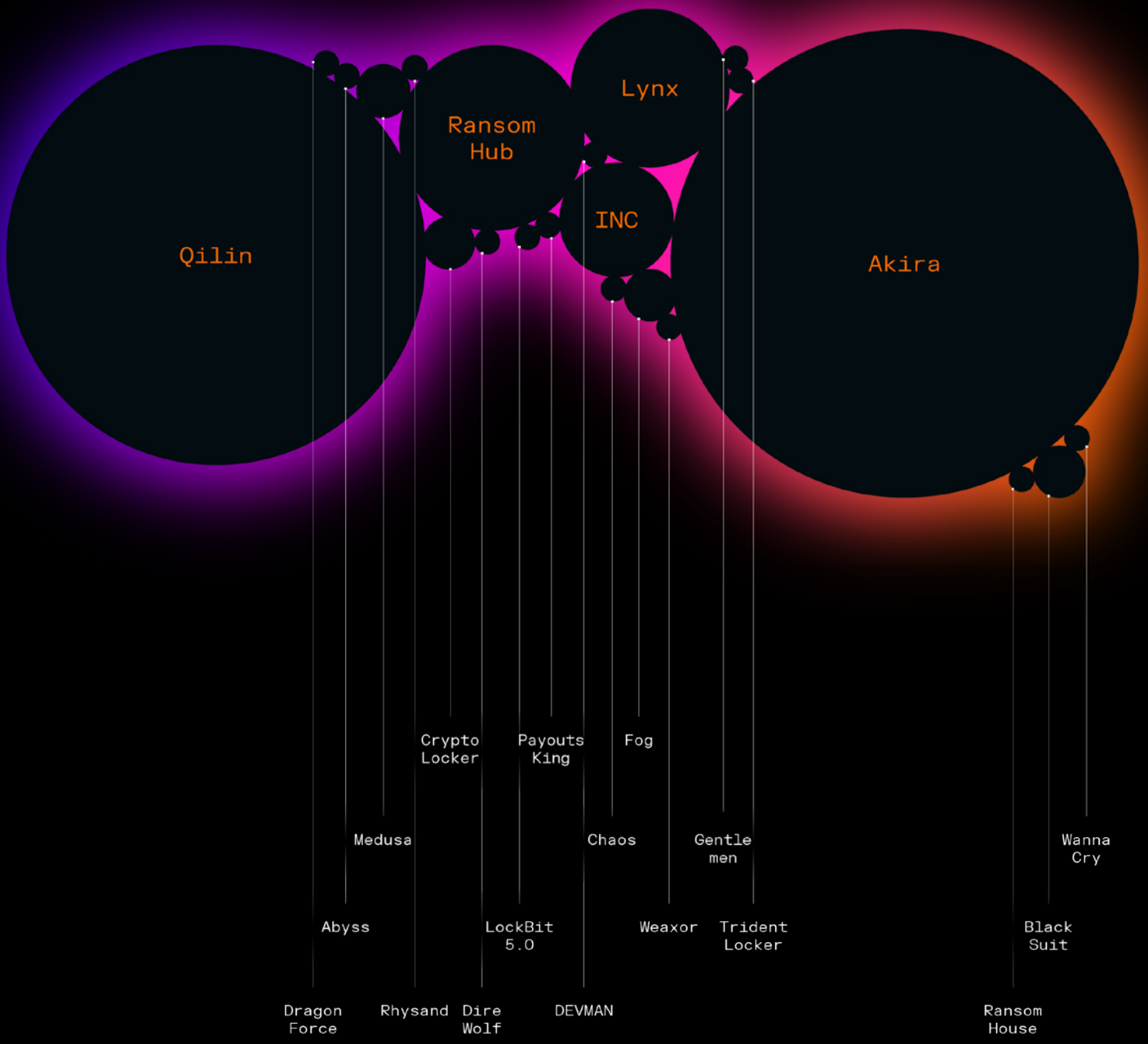
REACT2SHELL (CVE-2025-55182)

In December 2025, Darktrace researchers observed a rapid, opportunistic exploitation of CVE-2025-55182, a critical remote code execution vulnerability known as React2Shell.

Ransomware Trends & Analysis

The diagram below shows the top ransomware families observed in Darktrace incidents in 2025.

As defined in the methodology section in the appendix, cases were attributed to a specific ransomware strain or group where sufficient evidence was available, and attribution was based on observed encryption activity, including identifiable ransom note patterns or encryption file extensions; the presence of indicators of compromise (IoCs) associated with known ransomware groups; OSINT, typically derived from ransomware leaksite reporting; or confirmation provided directly by the affected customer.



Ransomware Trends & Analysis

Top five ransomware strains (excluding "Unknown", as defined in the Methodology section of the appendices) observed by Darktrace in 2025 include:

Akira
Qilin
RansomHub
Lynx
INC

THE TOP FIVE IN FOCUS

AKIRA
SonicWall SSL VPN exploitation with compromised credentials
VMware abuse
Lynx
Encrypting files with '.akira' extension
QILIN
RaaS group – significantly expanded in 2025
MSP [70] & supply chain access increases
Abuse of Windows Subsystem for Linux (WSL)-based encryptors
Gains access via phishing, exposed remote service credentials (through MSPs), conducts fast internal reconnaissance and lateral movement [71]. Abuses WSL to evade detection.
RANSOMHUB
In 2025, it matured into a stable, top-tier ransomware optimized for access, speed and extortion
Encrypting files with a mix of random numbe and characters
Facilitated remote access and scanning -> lateral movement -> data exfiltration
LYNX
Emerged as a rebrand/successor of INC
Encrypting files with ".LYNX" extension
Can shutdown VMs [72] to disrupt operations and make more complicated to recover
INC
Active since at least 2023
Encrypting files with ".INC" extension
Gains initial access via spear-phishing or vulnerabilities in Citrix NetScaler (CVE-2023-3519) [73]

Overview of Ransomware Cases by Month

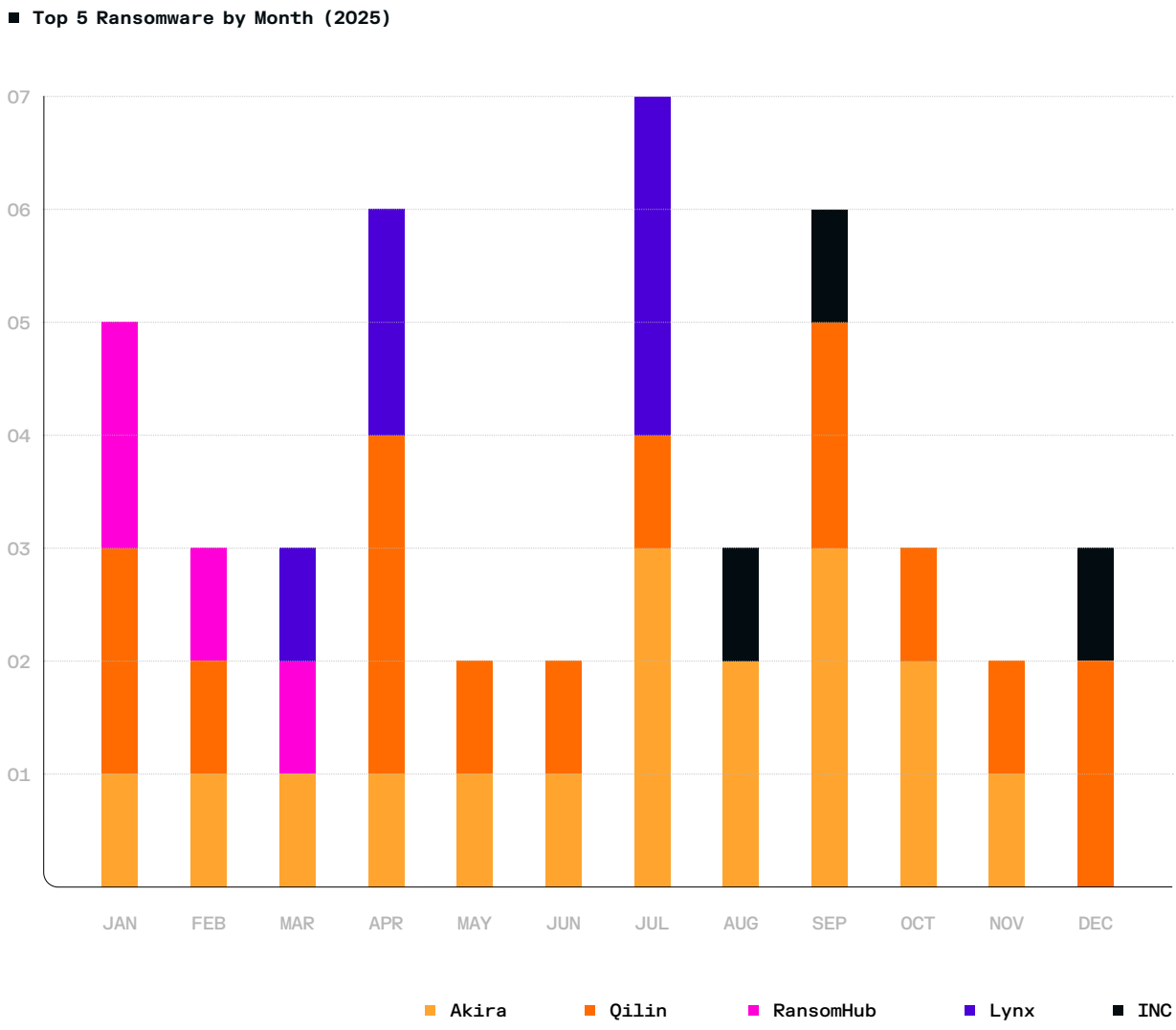
- **After emerging in early 2024,** RansomHub rapidly became one of the most prolific ransomware groups operating that year. Darktrace observed RansomHub activity from January through March 2025, but from the start of April 2025 the group was reported to have shut down their operations [74], with affiliates likely joining DragonForce and Qilin.
- **In April,** Darktrace observed three cases of Qilin ransomware that were likely linked to exploitation of a FortiGate vulnerability. OSINT reporting indicates that Qilin actors were seen exploiting multiple FortiGate vulnerabilities [75] in incidents between May and June.
- **From July to September,** Darktrace observed a higher number of Akira cases, most of which were related to exploitation of SonicWall appliances. Multiple OSINT reports around that time covered the same campaign [76, 77].

The vulnerabilities likely exploited by Akira and Qilin affiliates were not zero-days, demonstrating the need to patch quickly.

Overview of Ransomware Trends Across Sectors

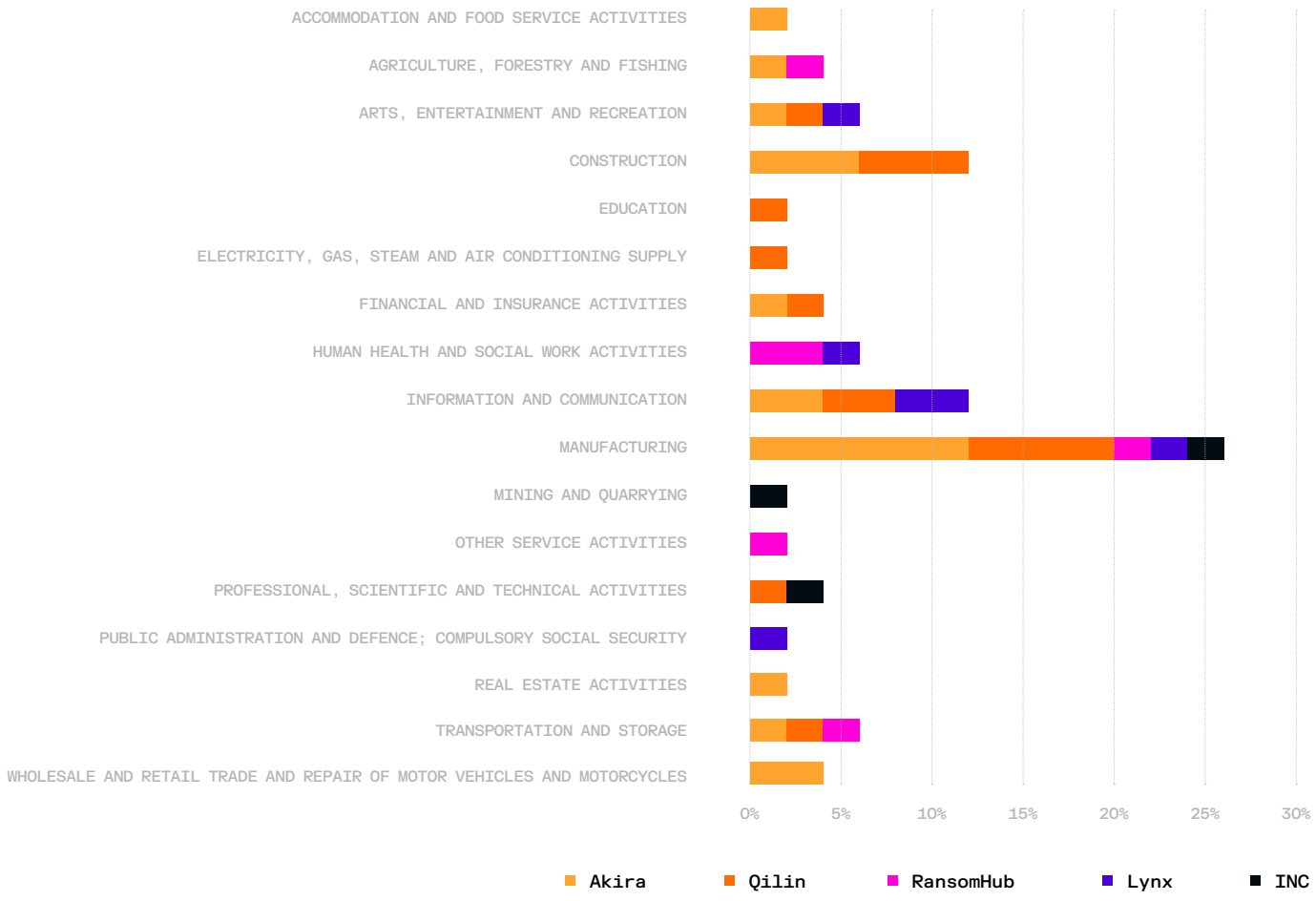
The top five sectors across the Darktrace fleet to be impacted by ransomware in 2025 were:

Manufacturing
Information and Communication
Construction
Human health and social work activities
Construction
Wholesale and retail trade and repair of motor vehicles and motorcycles



Breakdown of the overall top five most observed ransomware groups/strains

(Akira, Qilin, RansomHub, Lynx, INC) across each sector)



While there does not appear to be a clear sector preference for each ransomware group with cases distributed across a wide range of industries, Akira and Qilin do appear to commonly target companies in the Manufacturing and Construction sectors.

QILIN

- MANUFACTURING 25%
- CONSTRUCTION 19%
- INFORMATION AND COMMUNICATION 13%
- TRANSPORTATION AND STORAGE 7%
- PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES EDUCATION 6%
- REAL ESTATE ACTIVITIES 6%
- ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY 6%
- ARTS, ENTERTAINMENT AND RECREATION 6%
- FINANCIAL AND INSURANCE ACTIVITIES 6%
- EDUCATION 6%

AKIRA

- MANUFACTURING 33%
- CONSTRUCTION 17%
- INFORMATION AND COMMUNICATION 11%
- WHOLESALE AND RETAIL TRADE AND REPAIR OF MOTOR VEHICLES AND MOTORCYCLES 11%
- AGRICULTURE, FORESTRY AND FISHING 5%
- TRANSPORTATION AND STORAGE 5%
- ARTS, ENTERTAINMENT AND RECREATION 6%
- ACCOMMODATION AND FOOD SERVICE ACTIVITIES 6%
- FINANCIAL AND INSURANCE ACTIVITIES 6%

TTP Spotlight

ABUSE OF ADMINISTRATIVE/SERVICE CREDENTIALS IN AKIRA AND QILIN CASES

In almost half of the cases linked to Akira or Qilin, administrative or service credentials were found to be compromised and used for either initial access to a VPN environment or for lateral movement within the network.

These credentials often come with escalated privileges, allowing threat actors to access multiple devices or to transfer and execute files.

EDGE DEVICES

In 78% of Akira cases identified by Darktrace, the suspected entry vector was through an edge device such as a VPN gateway or firewall. Most of those cases involved a SonicWall appliance.

OTHER NOTABLE FINDINGS

- There were **two reported cases of BitLocker** being used to encrypt files. While BitLocker is a legitimate Microsoft Windows utility, there have been previous instances of it being abused by malicious actors to encrypt files and demand a ransom, such as the ShrinkLocker malware [78].
- Ransomware actors continue to abuse **RMM tools** for C2 communications or data exfiltration. These include AnyDesk, Splashtop, Atera, and RustDesk. Cloudflare tunnels were also seen in some cases, presumably for the same purposes.
- In the early phases of attacks, threat actors were also observed to use tools such as **Advanced IP Scanner, Advanced PortScanner, NetScan and Nmap** to perform scanning and reconnaissance.
- As the attacks progressed, the actors were commonly seen using **RDP or SSH** to move laterally across the network, often doing so with administrative credentials. LOTL techniques involving the use of PsExec and WinRM were also observed.
- During data gathering and exfiltration activity, Darktrace identified the following tools: **FileZilla, WinSCP, WinRAR, Rclone.**

In many cases, data was observed being exfiltrated to cloud storage or file sharing sites including MEGA, Limewire, Backblaze, Gofile, Filebin, and File[.]io.

Emerging Ransomware Strains of 2025

PAYOUTSKING [79, 80, 81]

- **Emerged** around mid-2025
- **Direct and double** extortion tactics
- **Claims to operate independently** (not as a RaaS affiliate) and conducts its own attacks to steal data and extort victims
- **Targeted countries:** Mainly US, Germany, France, and Spain
- **Observed TTPs:** As of now, no specific vulnerability or exploit has been disclosed. The group has published victim data on Tor-based leak sites, consistent with direct and double-extortion operations.

Targeted sectors:

Manufacturing
Healthcare
Construction
Agriculture and Food Production
Technology

DARKTRACE CASE STUDY:

- **No encryption** of files or a ransom note was observed.
- **An email was received from the threat actor** (similar to a ransom note) stating that the customer's data had been stolen
- **Initial access** may have been via a VPN

GENTLEMEN [82, 83, 84]

- **Identified** as a new ransomware operation that emerged around July-Aug 2025
- **Classic double-extortion** used
- **Targeted countries:** At least 17 countries; including Thailand, US, India, Mexico, and Colombia
- **Targeted sectors:** focusing heavily on a range of industries such as Manufacturing, Construction, Healthcare, Aviation, and Insurance
- **Observed TTPs:** Gains initial access by exploiting internet-facing services, including compromised FortiGate admin creds, and then performs internal recon (using Nmap or Advanced IP Scanner tools) and lateral movement. Heavily relies on legitimate admin tools like PsExec, WMI or PowerShell remoting. Data is staged and exfiltrated over encrypted SFTP using WinSCP. They also used Bring Your Own Vulnerable Driver (BYOVD) techniques at kernel level to terminate EDR/Defender products. Encrypts files with "7mtzhh" extension and drop ransom notes titled "README-GENTLEMEN[.]txt"

DARKTRACE CASE STUDY:

- Use of **Cloudflare** tunnels and **AnyDesk**
- **Download** of payloads from GitHub
- **Network scanning**, with evidence of NetScan usage
- Use of **compromised administrative credentials,** some evidence of bruteforcing
- **External RDP connections** to Flyservers
- **Connections** to penetration testing-related endpoints
- **Ransom note** 'README-GENTLEMEN.txt
- **Encrypted files** were appended with a randomly generated six-character alphanumeric extension

Darktrace SOC Trends & Analysis

The following insights from the Darktrace Security Operations Centre (SOC) highlight the most significant cyber threats that organizations faced in 2025 and are expected to persist into 2026 and beyond.

Exploitation of Edge Infrastructure for Initial Access

2025 was a record-breaking year for vulnerability disclosures. It is therefore no surprise that the Darktrace SOC identified threat actors frequently gaining initial access by exploiting vulnerabilities in edge infrastructure.

While some APT groups exploited zero-day vulnerabilities, others, such as the Akira ransomware group, leveraged long-since patched flaws, including CVE-2024-40766 in SonicWall SSL VPN appliances. Several more recently disclosed vulnerabilities were also exploited for initial access.

These included exploitation of Citrix NetScaler Gateway appliances via CitrixBleed 2 (CVE-2025-5777), SAP NetWeaver (CVE-2025-31324), and React2Shell (CVE-2025-55812), to name a few. As vulnerabilities continue to be identified at an increasing rate, this trend appears likely to continue into 2026.

Sophisticated Social Engineering Techniques

As users have become more aware of social engineering attacks, threat actors have continued to evolve their techniques. In 2025, attackers were observed leveraging modern social engineering tactics such as ClickFix to achieve their objectives.

Highly targeted social engineering campaigns were also observed, including spam bomb attacks followed by voice phishing attacks (vishing).

The Darktrace SOC identified threat actors using spam bombs to cause confusion and create a sense of urgency by flooding victims' inboxes with spam emails. Threat actors then followed up with voice phishing calls, impersonating IT teams to gain initial access.

These sophisticated and highly-targeted social engineering attacks were likely facilitated by the increased availability of AI tools such as large language models (LLMs). Such tools have lowered the barrier to entry for threat actors and enabled the creation of more customised and believable social engineering attacks.

Ransomware and Double Extortion

Double extortion ransomware, leveraging both data exfiltration and encryption, remained a common objective of threat actors in 2025.

Although some reports have suggested that ransomware groups are moving away from data encryption and increasingly focusing on data-theft-only extortion, Darktrace continued to observe multiple groups, **such as Akira, Qilin, and DragonForce, using a combination of data exfiltration and encryption to pressure victims into paying ransoms.**

The SOC's Monthly Breakdown

The table below highlights some of the most impactful and noteworthy threats affecting Darktrace customers, **tracked by Darktrace's SOC each month in 2025.**

JANUARY	FEBRUARY	MARCH
Initial Access through VPN (Fortinet)	Email Bombing	Ransomware
Remote Desktop Protocol abuse	Internal Proxy	QR Code Phishing
MintsLoader	Ransomware	DC Exploitation
Drive-by-Download	Entry via VPN (SonicWall)	Data Exfiltration
Ransomware	Cloud Infrastructure (AWS-based networks)	Account Manipulation (third-party file storage services)

APRIL	MAY	JUNE
Reverse Proxy Services	Edge Infrastructure Exploitation (SAP NetWeaver, Ivanti EPMM)	Tor Usage
Ransomware	Initial Access via Remote Services (VPN, VDI environments)	Alternative Phishing Techniques
Payment Diversion Fraud	Data Exfiltration	Automation in M365 Intrusions
Brute-Force Activity	VM Creation	Ransomware
Firewall Exploitation (Fortinet)	Payment Diversion Fraud	Payment Diversion Fraud

JULY	AUGUST	SEPTEMBER
Data Exfiltration (MEGA, MivoCloud)	UnPAC-the-hash Activity	Exfiltration from Salesforce
Ransomware	Double Extortion Ransomware	Ransomware Detonation
Reconnaissance Tools	SonicWall Firewall Exploitation	RMM Tool Usage
Remote Network Access Environments	Sophisticated Phishing Techniques	Abuse of Edge Infrastructure
Virtualized Environments	VPN Credential Abuse	Abuse of VPS Infrastructure

OCTOBER	NOVEMBER	DECEMBER
Edge Infrastructure Exploitation (WSUS, GoAnywhere MFT)	ClickFix Social Engineering	React2Shell
Hybrid Attacks (On-Premises & SaaS/Cloud)	Blockchain Abuse	C2 Implants (Sliver)
NetScan Scanning	Reconnaissance Tools (NetScan)	Cloud Attacks (Azure Kubernetes & Amazon S3 environments)
Legitimate Tool Abuse (PDQ Deploy, PsExec)	Ransomware	Group Policy Modification
Ransomware	Internet-Facing Devices	Ransomware

Campaign Activity Overview

Darktrace's Threat Research team investigates a range of threats affecting its customer base. Through this research, campaign-like clusters of activity have been identified, in which common TTPs, as well as infrastructure, are observed impacting a significant number of customers within a short timeframe.

The top five sectors across the Darktrace customer base affected by campaign clusters include:

- Manufacturing
- Education
- Information and communication
- Public administration and defence; compulsory social security
- Financial and insurance activities

Customers within EMEA formed over 50% of all those affected by campaigns.

Overall, customers across more than 30 different countries were affected by campaign activity identified by Darktrace's Threat Research team in 2025.

Atomic Information Stealer

Darktrace observed Atomic Stealer affecting customers worldwide in the second half of 2025, with activity peaking between June and October. In total, **customers in 27 countries across EMEA, AMS, and APJ were impacted.** Earlier cases were concentrated in EMEA and APJ, while the impact shifted toward a more balanced distribution across all three regions in later months. As noted in Darktrace's in-depth analysis of Atomic Stealer in 2025, the Education sector was the hardest hit, particularly in September and October 2025, as students returned to school. Earlier in the year, several other sectors were also significantly affected, including Financial and Insurance activities, Information and Communication, and Manufacturing.

While infostealer infections may not produce immediate or obvious effects, they can escalate into significant incidents if not swiftly detected and remediated by security teams. These risks include not only individual account takeovers, but also broader, network-wide threats such as ransomware. Indicators and network traffic patterns remained notably consistent throughout these campaigns, with C2 servers remaining within a single .0/24 CIDR range and URLs matching specific patterns [66].

The pervasiveness of this threat reflects the continued popularity of Malware-as-a-Service (MaaS), which also accounted for the majority of campaign activity within Darktrace's customer base in 2024 [61].

Vulnerability Exploitation

IVANTI

Continuing trends first seen in 2024 [67], Ivanti appliances remained widely targeted throughout 2025. The earliest signs of this activity emerged with the disclosure of two CVEs affecting Ivanti Connect Secure (CS) and Ivanti Policy Secure (PS) appliances. Darktrace's Threat Research team identified a small number of cases involving exploitation of CVE-2025-0282 and CVE-2025-0283, including one instance that occurred prior to the public disclosure of the CVEs. Ivanti exploitation had a more significant impact on Darktrace's customer base later in 2025, when two vulnerabilities affecting Ivanti Endpoint Manager Mobile (EPMM)—CVE-2025-4427 and CVE-2025-4428—were widely exploited by threat actors in May.

Among Darktrace customers specifically, those affected were primarily based in EMEA, with Germany the most impacted country and Manufacturing the most affected sector [68].

Post-exploitation activities in this case included delivery of the malware KrustyLoader, with similarities to exploitation of another critical vulnerability observed by Darktrace in the month prior; CVE-2025-31324 affecting SAP NetWeaver [69]. In both campaigns, KrustyLoader delivery was seen via rare AWS S3 bucket endpoints as well as some overlapping C2 infrastructure, with indications the activities may be associated with China-nexus threat actors.

REACT2SHELL

The most recent threat to affect a significant number of Darktrace customers was exploitation of React2Shell in December.

As detailed in Darktrace's recent blog, the Finance sector was significantly targeted during this campaign. Multiple customers within the Education sector were also targeted. The US was the most commonly targeted country, while countries across Africa accounted for the majority of the remaining targeting observed. The speed at which a public proof-of-concept was released provided an opportunity for a wide range of threat actors to exploit the vulnerability, including China-nexus and DPRK-affiliated actors attributed to distinct exploitation clusters, as well as others seeking financial gain.

Technological adoption in the US—particularly in cloud environments—has made it an attractive target for exploitation from both nation-state actors and financially-motivated attackers.

A subset of React2Shell exploitation was assessed as likely associated with DPRK threat actors, with specific payloads observed that support this attribution. Victims within this subset were primarily located in APJ, representing a notable shift from the broader and more geographically diverse React2Shell targeting observed overall.

Post-exploitation behavior revolved around the download of executable files or scripts in the majority of cases, with certain scripts recurring across multiple customers. Examples included scripts associated with the "Nuts and Bolts" campaign, as well as the script gfdsgsdfhfsd_ghsfdgsfdgsdfg.sh, described in further detail in this Darktrace blog published in December of last year.

Following the initial malware downloads, the attacks progressed through additional stages of the kill chain, including internal network scanning for reconnaissance, cryptomining activity, and C2 beaconing indicative of the abuse of red-teaming tools such as Sliver.

Part 03

Anomaly Detection in Action

Case Studies of Pre-CVE Detections in 2025

With a record-breaking, nearly 40,000 Common Vulnerabilities and Exposures (CVE) reported for 2024, 2025 surpassed that with a total of 48,185 CVEs published, representing a 20.6% increase year-on-year. The gap between exploitation of a zero-day and vulnerability disclosure can often be considerable, making retroactive identification of successful exploitation within networks a persistent challenge.

Abnormal behaviors within networks or systems, such as unusual login patterns or unexpected data transfers, can indicate attempted cyberattacks, insider threats, or compromised assets. As Darktrace does not rely on predefined rules or known signatures, it is able to detect malicious activity that deviates from established behavioral norms, even when full context about a specific device or asset is unavailable.

By continuously analyzing behavioral patterns, Darktrace enables organizations to identify and contain potential exploits at an early stage. Leveraging these anomaly detection parameters, Darktrace analysts conduct retrospective analysis to better understand detections across the broader threat landscape and to enrich findings with additional context. This behavioral approach also supports pre-CVE detection, allowing Darktrace to identify emerging or previously unknown exploitation techniques based on attacker behavior, before vulnerabilities are formally disclosed or assigned a CVE.

Darktrace demonstrated its ability to identify malicious activity prior to public disclosure in several notable cases throughout 2025, as outlined in the table below and further detailed in the appendix with corresponding model alert evidence.

For SAP NetWeaver (CVE-2025-31324), Darktrace detected anomalous behavior six days before the vulnerability was publicly disclosed, observing suspicious patterns indicative of exploitation attempts against Enterprise Resource Planning (ERP) systems.

Similarly, in the case of Ivanti CS, PS, and ZTA Gateways (CVE-2025-0282 and CVE-2025-0283), Darktrace identified unusual authentication activity and lateral movement weeks before Ivanti's official advisory, enabling early mitigation of attacks targeting remote access infrastructure.

Retrospectively, Darktrace identified model alerts related to CVE exploitation of Trimble Cityworks 18 days before disclosure while also having model alerts flag malicious activity even before that, demonstrating the benefit of behaviorial visibility of adversary activity targeting environments that support national level functions.

The affected environment sits within the CNI category due to its role in sustaining continuous aviation operations that underpin national mobility, emergency response, and defense logistics. Its integration with wider multimodal transport and logistics systems means any disruption could trigger cascading economic, operational, and security impacts, a defining characteristic of high-value CNI targets. The early detection window and the criticality of the operational environment underline both the strategic importance of the customer and the value of behavioral based detection ahead of formal vulnerability disclosure.

These examples underscore the value of behavioral AI in surfacing exploitation attempts before CVEs are published, reducing exposure windows and strengthening proactive defense.

CVE	CVE DISCLOSURE DATE (UTC)	DARKTRACE DETECTION DATE (UTC)	DAYS BETWEEN DARKTRACE DETECTION AND NIST CVE PUBLIC DISCLOSURE
CVE-2025-0282 (Ivanti Connect Secure/Policy Secure/ZTA)	2025-01-08	2024-12-29	11 days
CVE-2025-0283 (Ivanti Connect Secure/Policy Secure/ZTA)	2025-01-08	2024-12-29	11 days
CVE 2025-0994 (Trimble Cityworks)	2025-02-06	2025-01-19	18 days
CVE-2025-31324 (SAP NetWeaver)	2025-04-24	2025-04-18	6 days
CVE-2025-10035 (Fortra Go Anywhere MFT)	2025-09-18	2025-09-11	7 days

Part 04

Threat Actor Spotlights

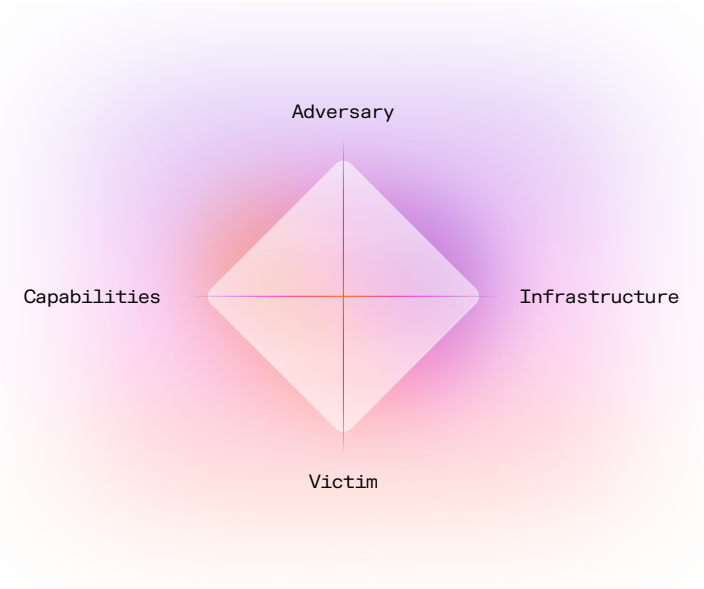


Figure 02: The Diamond Model of Intrusion Analysis

Understanding Salt Typhoon

Through the Diamond Model

Adversary

To better understand and analyze such adversary activities, security analysts and researchers widely use the Diamond Model of Intrusion Analysis, a cybersecurity framework designed for this purpose.

By applying the Diamond Model and combining it with Darktrace's capabilities, Darktrace's Threat Research team enhances its ability to understand the behavior of these persistent adversaries. This approach provides organizations with deeper insights and proactive defense strategies.

Salt Typhoon is a China-nexus cyber espionage threat cluster tracked by government and industry entities. Their strategic intent centers on establishing long-term, covert signals intelligence collection against global Telecommunications networks and other critical infrastructure to achieve advanced, persistent access.

In August 2025, the UK NCSC, alongside 12 allied nations, publicly linked three commercial organizations to Chinese intelligence services [88], highlighting both the malicious activity and the underlying state-contractor model enabling these operations to scale.

Infrastructure

Salt Typhoon predominantly targets telecommunications backbone and edge devices, whether provider or customer-owned, where firmware and configuration manipulation can grant long-term persistence with minimal defender visibility.

Tradecraft includes:

modifying access control lists

enabling SSH on non standard ports,

creating GRE tunnels and redirecting authentication services,

rapid exploitation of cloud data platforms

These techniques are described across multiple joint advisories published by the US Cybersecurity and Infrastructure Security Agency (CISA) [89]. Salt Typhoon also places consistent emphasis on exploiting known, patchable vulnerabilities in edge devices (e.g., Ivanti, Palo Alto, Cisco), reinforcing the pattern of compromises that should be avoidable.

Capabilities

Salt Typhoon is a highly capable cyber threat actor. Their initial access methods revolve around systemic exploitation of edge services, VPN interfaces, and router operating systems through well-known vulnerabilities that typically fall outside EDR visibility. **Their operational security is high, with persistence and stealth achieved through firmware or configuration tampering designed to survive reboots and evade host-based controls.**

Victim Profiling

Salt Typhoon primarily targets Telecommunications organizations, Government entities, Military institutions, and Transportation sectors—particularly within the US. In a 2025 intrusion against a European telecommunications provider, Darktrace observed dual channel C2 activity using LightNode infrastructure, as well as DLL sideloading paths delivering SnappyBee malware. Initial access is believed to have occurred via exploitation of a newly disclosed Citrix NetScaler vulnerability, consistent with previous reporting and the group's focus on moving from the network periphery to its core.

Understanding **Scattered Spider**

Through the Diamond Model

Adversary

Scattered Spider (also known as OctoTempest) is a financially-motivated, English-speaking cybercrime collective known for targeting large enterprises for extortion and ransom. Recent arrests in both the United States and United Kingdom highlight that significant cybercrime operations increasingly involve actors based in Western countries—previously considered less likely.

Initially associated with data theft and extortion in collaboration with other threat actors, Scattered Spider has also been observed deploying various ransomware strains, notably DragonForce.

Infrastructure

Scattered Spider excels at blending social engineering with cloud SaaS access, using these vectors to expand control during the leadup to ransoming an environment.

Their tactics include:

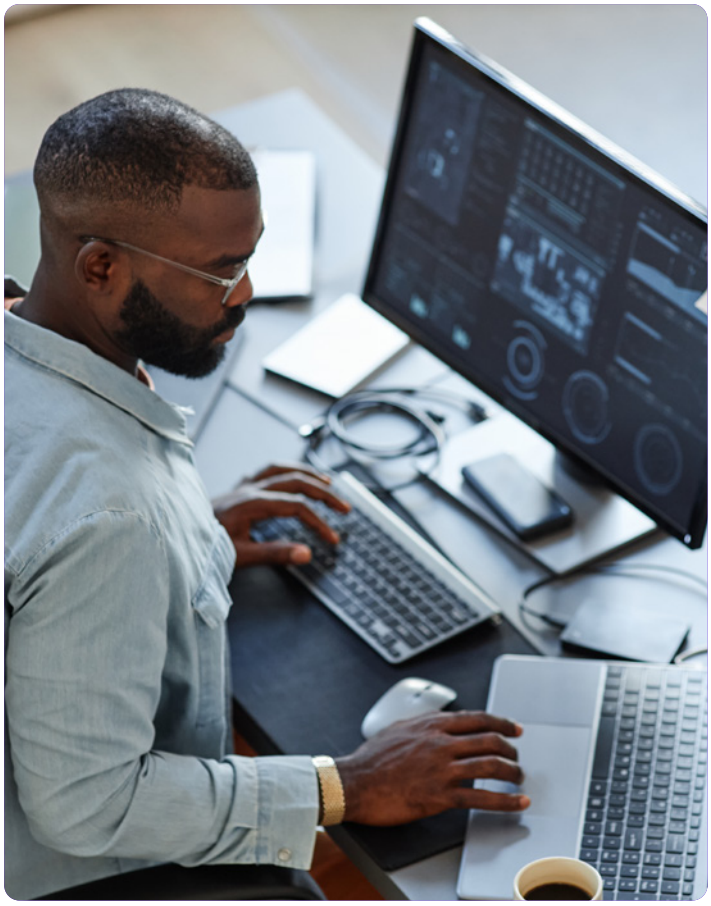
- help desk **impersonation**
- SIM-**swapping**
- MFA **abuse**
- **rapid exploitation** of cloud data platforms

These methods allow the group to create new identities and leverage proxy networks or rotating hostnames to obscure their activity. Darktrace has also observed victim-themed domains registered shortly before SIM-swapping attempts.

Capability

Phishing, MFA push bombing, and helpdesk impersonation are well-documented Scattered Spider techniques. The group frequently uses commercial remote access tools and LOTL methods to blend into normal operational activity. They are particularly adept at abusing commercial off-the-shelf platforms (e.g., Salesforce) once inside a victim environment to deepen access.

As a defense evasion tactic, Darktrace has observed Scattered Spider spinning up generic, unmanaged virtual machines as tooling hosts to bypass EDR controls, installing tools such as AnyDesk to establish persistent, VPN independent access. These methods enable sustained lateral movement and credential harvesting, forcing defenders into challenging containment decisions.



Victim Profiling

Scattered Spider typically targets large, well-known commercial organizations. Enterprises that heavily outsource helpdesk functions or rely extensively on SaaS services are particularly at risk.

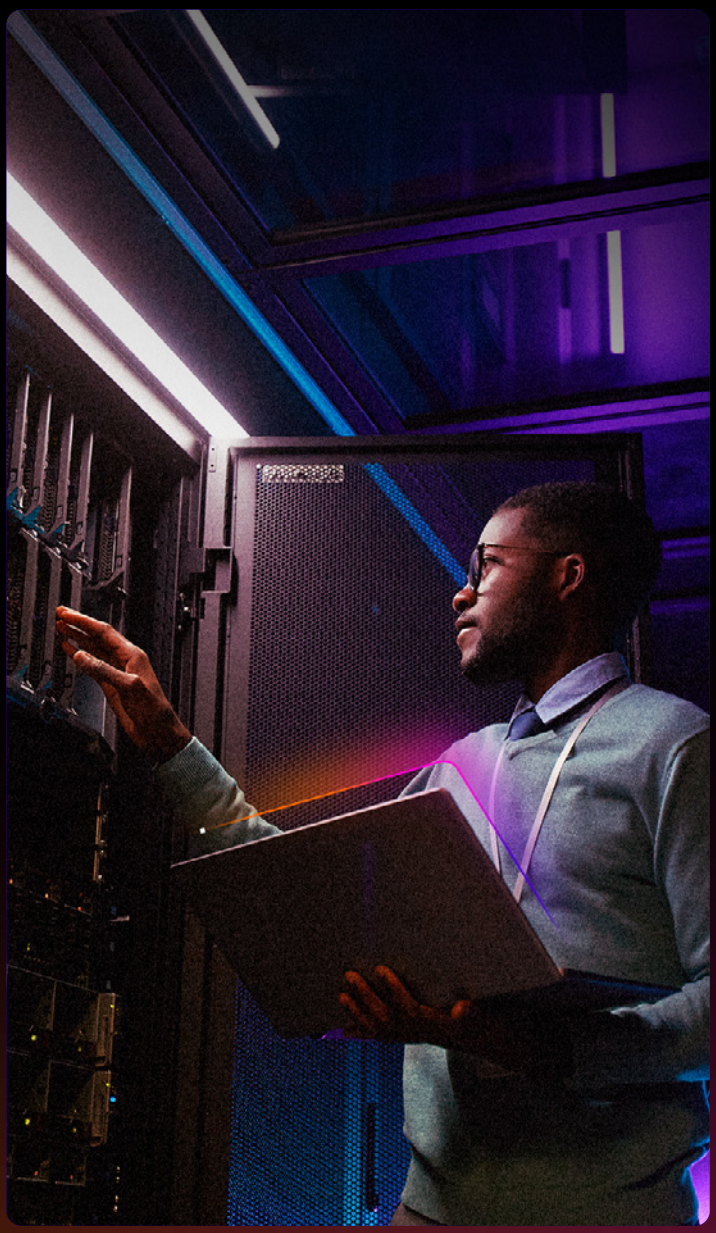
In 2025, Scattered Spider was widely considered responsible for the United Kingdom's costliest cyberattack on record—estimated at GBP 1.9 billion [90].

Darktrace's summer 2025 investigations into Scattered Spider attacks highlighted identity-first intrusions, widespread LOTL activity, and increased use of RaaS, aligned with reporting from national cyber agencies such as CISA.

Part 05

Outlook for 2026

Looking ahead to 2026, cyber risk will be shaped less by isolated incidents and more by systemic exposure across identities, cloud control planes, and interconnected software supply chains. There are five trends to watch over the next year:



01 RANSOMWARE
will remain the fastest path to material business impact. It will be increasingly enabled by identity abuse, email-based manipulation, and legitimate cloud access rather than bespoke malware.

02 VULNERABILITY VOLUME
and time to exploitation outpaces remediation capacity. The expanding volume of disclosed vulnerabilities will continue to stretch security and engineering teams, underscoring the limits of patch-centric defense models. As vulnerability growth outpaces remediation capacity, organizations will need to prioritize based on exploitability, exposure, and behavioral indicators—not raw severity scores. Pre-CVE abuse, configuration drift, and credential compromise are likely to remain dominant breach vectors, accelerating the shift toward detecting malicious intent and anomalous use of legitimate permissions.

03 SAAS PLATFORMS BECOME HIGHER IMPACT SUPPLY CHAIN TARGETS

As attackers aim for scale and efficiency, SaaS platforms are becoming preferred supply chain targets, offering disproportionate downstream impact when compromised. Highly trusted, deeply integrated SaaS applications provide adversaries access to multiple environments through a single foothold—often via valid credentials, APIs, or subtle misconfigurations that evade traditional security controls.

04 GENERATIVE AI-ENABLED CYBERCRIME
becomes commercialized and productized. At the same time, the commercialization of generative AI-enabled cybercrime is accelerating. Techniques that lowered the barrier to entry in 2025 are becoming productized in 2026, with AI-assisted playbooks and prompt-driven attack frameworks openly traded in criminal ecosystems. The combination of AI-driven automation and trusted SaaS abuse enables threats that are more scalable, reusable, and difficult to distinguish from legitimate activity—further eroding assumptions about trust, tooling, and supply chain integrity.

05 INCREASED TARGETING AND FOCUS ON CNI
Nation-state and hybrid actors will deepen their focus on critical national infrastructure and strategically important sectors, exploiting interconnected vendors and service ecosystems to achieve persistence and operational freedom. In this environment, resilience in 2026 will depend on the ability to constrain trust through least privilege principles, continuously monitor identity and cloud behavior for subtle deviations, and recover at business speed—accepting that vulnerabilities are inevitable, but undetected abuse is not.

Part 06

Appendices

Methodology

Darktrace's Threat Research Methodology

Darktrace's Threat Research team conducts extensive research across customer deployments to identify active threats, pinpoint key IoCs, and provide relevant threat intelligence. This research leverages Darktrace's anomaly-based detection and involves thorough analysis and contextualization by the Threat Research team. Detected threats are promptly reported to the relevant customer security teams. When a customer has Darktrace's Autonomous Response technology enabled, these threats are swiftly mitigated to prevent escalation.

Between January 1 and December 31, 2025, Darktrace investigated a wide range of cyber threats across its customer base. Many were identified as campaign-like activities targeting multiple customers, where clusters of similar TTPs and IoCs were seen affecting a significant number of customers within a short timeframe. Statistics within the 'Campaign Activity Overview' section were derived based on identified campaign clusters as described. All insights from Darktrace's analysis are based on detections and specific data from our AI-driven applications and anomaly investigations.

Sector Analysis Methodology

Throughout this report, sectors and industries are defined using the Standard Industrial Classification (SIC) system to ensure a consistent and standardized approach to categorizing organizations. To ensure clarity and consistency throughout the report, sector and industry category names are capitalized when used as defined classifications. Additionally, when considering insights and statistics relating to sectors in this report, it is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the distribution of Darktrace customers across different sectors. For example, the Finance, Manufacturing, and Education sectors are prominent within Darktrace's customer base, increasing the likelihood of a higher number of observed cases. This is expected and does not necessarily indicate increased sector-specific risk.

Regional Analysis Methodology

When considering the insights presented in the Regional Breakdown sections of this report, 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. Similarly, in Latin America, Darktrace has a higher concentration of customers in Colombia than in other countries, increasing the likelihood of observing a greater number of cases there. While customer distribution influences these findings, the activity observed in Colombia is also consistent with broader regional and global targeting trends.

SOC Trends Methodology

The observations in the 'A View from the SOC' section of this report are based on high-fidelity inputs analyzed through Darktrace's Managed Threat Detection and Security Operations Support services. This analysis, conducted between January 1 and December 31, 2025, involves both pattern analysis and assessment of data significance. These insights are primarily qualitative and reflect our SOC team's evaluation of the most significant cyber threats in 2025.

Email Trends and Analysis Methodology

The statistics highlighted in the 'Email Trends and Analysis' section are derived from analysis of monitored Darktrace / EMAIL model data for all customer deployments hosted in the cloud between January 1, 2025, and December 31, 2025, with subsets of these deployments used to derive statistics for specific geographical regions. Please note that data for June 2025 was unavailable for analysis. Around 90% of the global Darktrace customer base's email environments are cloud-based. For the purpose of this report, and indeed Darktrace's analysis of email environments, "phishing indicators" refers to emails that are confirmed as malicious, as opposed to merely unwanted spam emails, while "phishing emails" refers to emails containing "phishing indicators". Discussion of Black Friday phishing trends refers to emails containing Black Friday terminology in combination with phishing indicators. When referring to brand abuse of Global consumer vendors and United States consumer vendors within email threats we refer specifically to phishing emails involving abuse of the following brands: Global Consumer Vendors Amazon, eBay, Netflix, Alibaba, PayPal, Apple, and United States Consumer Vendors Walmart, Target, Best Buy, Macy's, Old Navy, 1-800 Flowers. Historic analysis has found these brands to be among the most commonly impersonated.

Ransomware Analysis Methodology

In the ransomware analysis presented in this report, cases were attributed to a specific ransomware strain or group where sufficient evidence was available. Attribution was based on observed encryption activity, including identifiable ransom note patterns or encryption file extensions; the presence of indicators of compromise (IoCs) associated with known ransomware groups; OSINT, typically derived from ransomware leaksite reporting; or confirmation provided directly by the affected customer. Cases for which the available evidence was insufficient to support reliable attribution were classified as "Unknown" and were excluded from any analysis.

Bibliography

[1] [Online]. Available: https://www.feedzai.com/blog/latam-financial-regulations/.

[2] [Online]. Available: https://hackenproof.com/blog/for-business/crypto-regulations-latin-america-2025-2026.

[3] [Online]. Available: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market.

[4] [Online]. Available: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/latin-america .

[5] [Online]. Available: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market.

[6] [Online]. Available: https://www.enisa.europa.eu/news/whats-driving-cybersecurity-investments-and-where-lie-the-challenges.

[7] [Online]. Available: https://www.ncsc.gov.uk/news/ncsc-issues-warning-over-hacktivist-groups-disrupting-uk-organisations-online-services.

[8] [Online]. Available: https://dtpgroup.co.uk/insight/50-cloud-computing-statistics.

[9] [Online]. Available: https://www.bankinfosecurity.com/cloud-identity-exposure-a-critical-point-failure-a-29924.

[10] [Online]. Available: https://sitsi.pacanalyst.com/part-6-cloud-security-shared-responsibility-and-real-accountability/.

[11] [Online]. Available: https://industrialcyber.co/reports/businesses-and-manufacturing-bear-brunt-of-36-ransomware-spike-as-government-and-health-care-see-declines/.

[12] [Online]. Available: https://minipip.co.uk/details/news/jaguar-land-rover-cyber-attack-costs---200-million-and-hits-uk-gdp.

[13] [Online]. Available: https://www.gov.uk/government/calls-for-evidence/financial-services-growth-and-competitiveness-strategy/outcome/financial-services-growth-and-competitiveness-strategy-overview.

[14] [Online]. Available: https://transfer.lc/french-retail-market/.

[15] [Online]. Available: https://www.chooseparisregion.org/industries/fashion-luxury.

[16] [Online]. Available: https://www.kelacyber.com/wp-content/uploads/2022/10/KELA-RESEARCH_France-Threat-Landscape-Report_-Luxury-Industry.pdf.

[17] [Online]. Available: https://www.symmetry-systems.com/blog/what-we-know-so-far-about-salesloft-and-other-recent-salesforce-breaches/.

[18] [Online]. Available: https://www.securityweek.com/hundreds-of-thousands-affected-by-auchan-data-breach/.

[19] [Online]. Available: https://cloudprotection.com/blog/salesforce-attacks-in-2025/.

[20] [Online]. Available: https://www.gtai.de/en/invest/business-location-germany/market-germany-europe-s-economic-hub#toc-anchor—1.

[21] [Online]. Available: https://senzemo.com/iot-solutions-for-the-german-market-key-industry-conferences.

[22] [Online]. Available: https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year.

[23] [Online]. Available: https://www.dw.com/en/china-puts-pressure-on-german-car-chemicals-engineering-industry/a-71919309.

[24] [Online]. Available: https://www.sophos.com/en-gb/research/shadowpad-malware-analysis.

[25] [Online]. Available: https://www.darktrace.com/blog/nis2-compliance-interpreting-state-of-the-art-for-organisations.

[26] [Online]. Available: https://www.logisticsit.com/articles/2023/07/05/a-look-at-new-in-the-nis2-directive?__cf_chl_tk=gKfPKYT7K1P1OMr-RMIEzWO6LDFFt35OPyE6_bZ359vo-1768949517-1.0.1.1-0IZrxZJ4_zcMFBoc4dyBuSK0NyBSYIf65t6FtFDeUEc.

[27] [Online]. Available: https://secomea.com/blog/compliance/nis2-scope-essential-important-entity/.

[28] [Online]. Available: https://www.darktrace.com/resources/7-steps-to-get-ahead-with-nis2.

[29] [Online]. Available: https://www.darktrace.com/blog/modernising-uk-cyber-regulation-implications-of-the-cyber-security-and-resilience-bill.

[30] [Online]. Available: https://www.darktrace.com/blog/uk-cyber-security-and-resilience-bill-what-it-means-for-organizations .

[31] [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757633/EPRS_BRI(2024)757633_EN.pdf.

[32] [Online]. Available: https://www.youtube.com/watch?v=7CVz57sLVPw&t=15s.

[33] [Online]. Available: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en.

[34] [Online]. Available: https://www.theglobalcity.uk/insights/thought-pieces/scaling-digital-verification-solutions.

[35] [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa.

[36] [Online]. Available: https://www.uneca.org/cybersecurity-for-development-in-the-fourth-industrial-revolution-research-report.

[37] [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_GCIv2_report.pdf.

[38] [Online]. Available: https://www.darktrace.com/blog/unmasking-vo1d-inside-darktraces-botnet-detection .

[39] [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23779497.2025.2532556?src=#d1e121 .

[40] [Online]. Available: https://thehackernews.com/2025/03/vo1d-botnets-peak-surpasses-159m.html .

[41] [Online]. Available: https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/Vo1d-rising-inside-the-botnet-controlling-168M-Android-TVs-worldwide.pdf .

[42] [Online]. Available: https://mybroadband.co.za/news/broadcasting/596007-warning-for-south-africans-using-specific-types-of-tv-sticks.html.

[43] [Online]. Available: https://www.securityweek.com/vo1d-botnet-evolves-as-it-ensnares-1-6-million-android-tv-boxes/ .

[44] [Online]. Available: https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/ .

[45] [Online]. Available: https://industrialcyber.co/features/growing-convergence-of-geopolitics-and-cyber-warfare-continue-to-threaten-ot-and-ics-environments-in-2024/.

[46] [Online]. Available: https://www.congress.gov/crs_external_products/R/PDF/R48067/R48067.12.pdf.

[47] [Online]. Available: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf .

[48] [Online]. Available: https://phr.org/our-work/resources/occupied-hospitals-and-surgery-in-the-dark-ukraine/.

[49] [Online]. Available: https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf.

[50] [Online]. Available: https://mccraryinstitute.com/app/uploads/2025/10/McCrary-Institue-Code-Red-Release-Ready.pdf.

[51] [Online]. Available: https://www.utilitydive.com/news/china-energy-utility-cyber-threat-typhoon/806893/.

[52] [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat.

[53] [Online]. Available: https://www.theregister.com/2025/02/14/chinese_spies_ransomware_moonlighting/.

[54] [Online]. Available: https://www.darktrace.com/blog/unpacking-clickfix-darktraces-detection-of-a-prolific-social-engineering-tactic.

[55] [Online]. Available: https://reliaquest.com/blog/threat-spotlight-attackers-exploit-axios-for-automated-phishing/.

[56] [Online]. Available: https://www.hipaajournal.com/patient-death-linked-to-ransomware-attack/.

[57] [Online]. Available: https://hyperproof.io/resource/understanding-the-change-healthcare-breach/.

[58] [Online]. Available: https://blog.barracuda.com/2025/05/16/cl0p-ransomware--the-skeezy-invader-that-bites-while-you-sleep.

[59] [Online]. Available: https://www.darktrace.com/resources/the-state-of-cybersecurity-in-the-finance-sector.

[60] [Online]. Available: https://www.cyberdefensemagazine.com/the-ot-cybersecurity-challenge-navigating-the-journey-to-a-secure-industrial-future/.

[61] [Online]. Available: https://www.darktrace.com/resources/annual-threat-report-2024 .

[62] [Online]. Available: https://blog.barracuda.com/2025/08/20/threat-spotlight-split-nested-qr-codes-quishing-attacks .

[63] [Online]. Available: https://www.infosecurity-magazine.com/news/hackers-qr-codes-new-quishing/ .

[64] [Online]. Available: https://www.darktrace.com/blog/phishing-attacks-surge-by-620-in-the-lead-up-to-black-friday .

[65] [Online]. Available: https://www.darktrace.com/blog/from-amazon-to-louis-vuitton-how-darktrace-detects-black-friday-phishing-attacks .

[66] [Online]. Available: https://www.darktrace.com/blog/atomic-stealer-darktraces-investigation-of-a-growing-macos-threat.

[67] [Online]. Available: https://www.darktrace.com/blog/darktraces-early-detection-of-the-latest-ivanti-exploits.

[68] [Online]. Available: https://www.darktrace.com/blog/ivanti-under-siege-investigating-the-ivanti-endpoint-manager-mobile-vulnerabilities-cve-2025-4427-cve-2025-4428.

[69] [Online]. Available: https://www.darktrace.com/blog/tracking-cve-2025-31324-darktraces-detection-of-sap-netweaver-exploitation-before-and-after-disclosure.

[70] [Online]. Available: https://thehackernews.com/2025/11/qilin-ransomware-turns-south-korean-msp.html .

[71] [Online]. Available: https://thehackernews.com/2025/10/qilin-ransomware-combines-linux-payload.html .

[72] [Online]. Available: https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/.

[73] [Online]. Available: https://www.trendmicro.com/vinfo/gb/security/news/ransomware-spotlight/ransomware-spotlight-inc.

[74] [Online]. Available: https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html.

[75] [Online]. Available: https://securityaffairs.com/178736/hacking/attackers-exploit-fortinet-flaws-to-deploy-qilin-ransomware.html .

[76] [Online]. Available: https://arcticwolf.com/resources/blog-uk/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn-copy/ .

[77] [Online]. Available: https://www.theregister.com/2025/09/10/akira_ransomware_abusing_sonicwall/ .

[78] [Online]. Available: https://securelist.com/ransomware-abuses-bitlocker/112643/.

[79] [Online]. Available: https://www.linkedin.com/pulse/creditinfo-lietuva-ransomware-breach-payoutsking-2025-girdziu%C5%A1as--azgaf .

[80] [Online]. Available: https://www.ransomware.live/group/payoutsking .

[81] [Online]. Available: https://www.comparitech.com/news/rehab-clinics-in-jacksonville-fl-targeted-by-new-ransomware-gang/ .

[82] [Online]. Available: https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html .

[83] [Online]. Available: https://www.cybereason.com/blog/the-gentlemen-ransomware .

[84] [Online]. Available: https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2025/11/kpmg-ctip-gentlemen-ransomware-11-nov-2025.pdf.coredownload.inline.pdf .

[85] [Online]. Available: https://www.cloudzero.com/blog/cloud-computing-statistics/.

[86] [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/.

[87] [Online]. Available: https://spacelift.io/blog/cloud-security-statistics.

[88] [Online]. Available: • https://www.ncsc.gov.uk/pdfs/news/uk-allies-expose-china-tech-companies-enabling-cyber-campaign.pdf.

[89] [Online]. Available: • https://www.cisa.gov/news-events/alerts/2025/08/27/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise.

[90] [Online]. Available: https://www.bbc.co.uk/news/articles/cy9pdld4y81o.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

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