ANNUAL THREAT PULSE REPORT

2025

DigitalXRAID
a XYPHER company

Executive Summary

2025 was a more disruptive, stealthy, and systemic year for cyber threats. Attackers didn't need more malware, more exploits, or more noise to achieve impact. Instead, they focused on abusing identity, trust, and dependency.

The result was a year defined by operational disruption, prolonged dwell time, and incidents that spread far beyond the initially compromised organisation.

Across the year, the DigitalXRAID monthly Threat Pulse observed a clear shift away from opportunistic, high volume attacks towards precise campaigns designed to maximise leverage:

- Identity systems became the primary entry point.
- SaaS platforms and supply chains amplified impact.
- Ransomware evolved into an extortion and disruption model where encryption was optional.
- Public services, manufacturing, healthcare, and critical suppliers carried a disproportionate share of the risk.

This marks a fundamental change in how cyber risk should be understood. Cyber incidents in 2025 were business continuity crises, safety risks, and governance issues. The organisations that struggled most weren't those without tools – on the contrary, some of the worst hit had tooling in place - but those without visibility, readiness, and rehearsed response.

Key Findings

The most significant finding of 2025 is a shift from volume to impact. While the number of attacks remained high, the defining characteristic of the year was how damaging individual incidents became.

2025: The year attackers stopped breaking in, and started logging in.

Identity abuse, supply-chain compromise, and operational disruption emerged as the dominant themes. Attackers consistently bypassed traditional controls by exploiting people, processes, and trusted platforms, rather than focusing on technical vulnerabilities.

Ransomware remained the most common threat, but its role has changed. Encryption was often unnecessary. Data theft, service disruption, and reputational pressure were enough to force negative outcomes.

Key Threat Trends in 2025

- Ransomware remained persistent, but attacker focus shifted from encryption to data theft, extortion, and operational disruption.
- Identity abuse became the primary initial access vector, overtaking malware and exploit-led intrusion.
- Supply-chain and SaaS compromises created the largest and fastest spreading incidents, with a single breach impacting many organisations.
- Manufacturing, healthcare, retail and public sector organisations were the most consistently targeted due to high disruption value and low tolerance for downtime.
- Living-off-the-land and malware-free techniques reduced detection visibility and increased dwell time.
- DDoS and service disruption were increasingly used as politically aligned pressure tools, not just criminal nuisance attacks.
- High and Critical vulnerabilities were exploited rapidly, with patch latency becoming a major risk factor.
- Prevention controls alone proved insufficient, reinforcing the need for resilience, visibility, and rehearsed incident response.

Together, these trends show a threat landscape that is quieter, more patient, and more strategically aligned to business impact.

Most Severe Threat of 2025

The most severe threat observed in 2025 was identity led ransomware and extortion campaigns that caused operational shutdown.

These campaigns didn't rely on novel malware or complex exploits. They relied on compromised credentials, help desk impersonation, token abuse, and trusted access paths. Once inside, attackers blended into normal activity, exfiltrated data, and applied pressure through disruption rather than encryption.

The defining example of this was the ransomware driven disruption at Jaguar Land Rover, where attacker access led to production outages and operational impact across manufacturing operations. The incident is cited as the most economically damaging cyber event to ever happen in the UK with £1.9 billion of financial loss. It demonstrated how identity compromise can cascade rapidly into business interruption, even in organisations with mature technical security controls.

For manufacturing and public services sectors, downtime carries immediate financial, safety, and societal consequences. Attackers exploited this pressure, knowing that even limited disruption could force rapid decisions.

Why This Threat Matters

The impact goes beyond IT systems.

Business continuity is directly affected when production lines stop, services are unavailable, or suppliers are disrupted. Safety and availability risks increase in environments where digital systems underpin physical operations or public services. Regulatory exposure grows as incidents affect personal data, essential services, and reporting obligations under UK and EU frameworks.

This reinforces a critical lesson from 2025: the most damaging attacks weren't technically loud, but operationally decisive. Identity compromise combined with targeted disruption proved more effective than widespread encryption, making resilience and response readiness as important as prevention.

From 2024 to 2025: What Changed, What Didn't?

In 2024, the dominant drivers were volume and speed. Attackers favoured new ransomware strains, mass phishing, and rapid exploitation. Malware was visible, attacks were noisy, and monetisation was fast.

In 2025, those drivers matured. Attackers reused tools, abused trust, and focused on access, persistence, and leverage. The escalation wasn't about scale, but about improving the effectiveness of their attacks. This represents a maturity shift in attacker behaviour rather than a simple increase in threat levels.

Implications and Recommendations

The implications for boards and senior leaders are clear. Cyber risk must be treated as an operational and governance issue, not just a technical one. Visibility across identity, cloud, and suppliers is as important as endpoint protection. Resilience planning and decision readiness are critical when prevention is bypassed.

Organisations should expect incidents to involve third parties, legitimate platforms, and prolonged uncertainty. Governance, communication, and response capability are as important as controls.

Key Recommendations for 2026

2025 demonstrated that attackers no longer need to break systems to break organisations.

Preparing for 2026 means accepting that reality and building the capability to respond when trust, access, and operations are under pressure.

Key recommendations:

- Prioritise identity-first security, including conditional access, token controls, and monitoring of abnormal identity behaviour.
- Harden help desk and account recovery processes against impersonation and social engineering.
- Treat SaaS platforms and suppliers as core components of the attack surface, not external risks.
- Reduce patch latency for high and critical vulnerabilities, especially on edge and identity systems.
- Invest in visibility across cloud, identity, and data movement, not just endpoints.
- Strengthen incident response planning, including executive and operational table-top exercises.
- Test backup, recovery, and continuity plans under realistic disruption scenarios.
- Align cyber security governance with operational risk, regulatory obligations, and business resilience.

Top 10 Findings

2025 proved that cyber risk is no longer measured by how many attacks you face, but by how much damage a single intrusion can cause. Across the Threat Pulse updates, ten themes stood out consistently.

- Ransomware remained the most common threat, but extortion and data theft became more central. Attackers increasingly used data exposure, deadlines, and business pressure as the primary leverage, even when encryption never occurred.
- Identity attacks were the most repeatable entry path. Help desk impersonation, phishing, OAuth abuse, and token theft repeatedly enabled access without needing malware or complex exploitation.
- SaaS and third-party compromise created the largest blast radius. A single vendor breach or token compromise could expose hundreds of downstream environments, shifting risk from individual organisations to entire ecosystems.
- All CVEs referenced were High or Critical, and nearly half were Critical. This reinforces a simple reality: attackers focused on the most easily weaponised, high impact flaws, and exploited them quickly when patching lagged.
- Manufacturing, healthcare, retail and public sector organisations were the most consistently targeted. These sectors combine high operational dependency, limited tolerance for downtime, and complex supplier relationships, making them ideal extortion targets.
- Operational disruption became a core attacker outcome, not just a side effect. Production halts, service outages, transport disruption, and public service impacts appeared alongside data theft, and sometimes replaced it entirely.
- DDoS scaled significantly and became more geopolitically aligned. Disruption was increasingly used as a pressure tool linked to political events, conflict narratives, and hacktivist campaigns, not just criminal opportunism.
- UK cyber intensity increased sharply, with CNI and suppliers under sustained pressure. The pattern across 2025 points to heightened targeting of essential services and the organisations that support them, increasing regulatory and resilience expectations.
- Malware-free and living-off-the-land tactics increased detection difficulty. Attackers relied more on legitimate tools and native admin functions, blending into normal activity and reducing the effectiveness of signature-led detection.
- AI-assisted and socially engineered attacks became increasingly operationalised. AI was used to improve phishing quality, scale reconnaissance, and enable more convincing fraud and extortion narratives, including deepfake-driven scenarios.

Introduction to the 2025 Cyber Security Landscape

The cyber threat landscape in 2025 continued to evolve, but not in the way many organisations expected.

While attack volumes remained high, the defining characteristics of the year were increased precision, deeper impact, and a clear shift towards stealth and leverage. Attackers relied less on noisy malware and more on automation, identity abuse, and trusted infrastructure to gain access and remain undetected. AI assisted techniques, improved social engineering, and living off the land tactics allowed threat actors to bypass traditional controls and operate with a longer dwell time inside victim environments.

Rather than chasing novelty, adversaries refined what worked. Identity systems, SaaS platforms, cloud control planes, and supply chains became the preferred routes in. Operational disruption emerged as a deliberate outcome, not just a side effect of data theft or ransomware.

The result was fewer obvious warning signs, much longer dwell times, and incidents that impacted safety, service delivery, and public trust as much as confidentiality.

Most Common Cyber Threats

Across 2025, several threat categories appeared repeatedly, often evolving in form rather than disappearing.

Ransomware and extortion remained the most persistent threat. While encryption was still used, many campaigns prioritised data theft, operational pressure, and reputational leverage over locking systems.

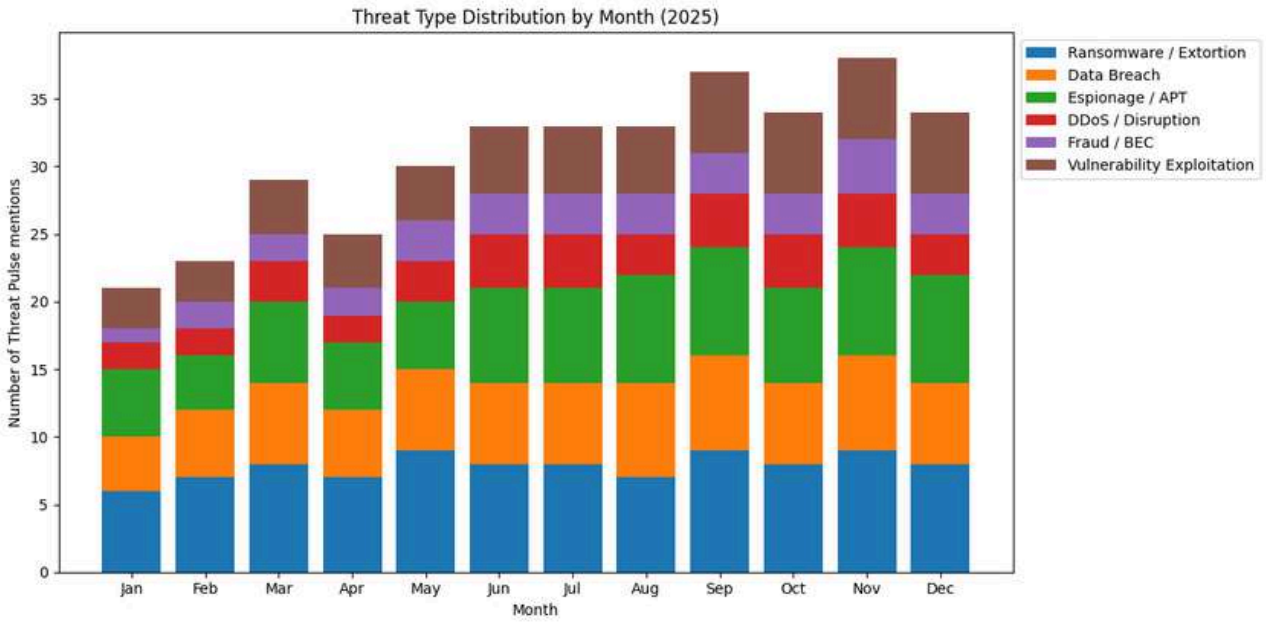
Data breaches featured heavily, particularly those linked to SaaS platforms, cloud services, and third-party providers. In many cases, data exposure occurred without malware deployment or encryption.

Espionage and advanced persistent threat activity continued throughout the year, driven by geopolitical tensions and focused on government, technology, manufacturing, and critical infrastructure.

DDoS and disruption events increased in scale and visibility. These attacks were frequently linked to political narratives, hacktivist campaigns, or attempts to disrupt services rather than extract ransom.

Fraud and business email compromise evolved rapidly, with AI assisted social engineering, deepfake techniques, and OAuth abuse enabling high value financial losses.

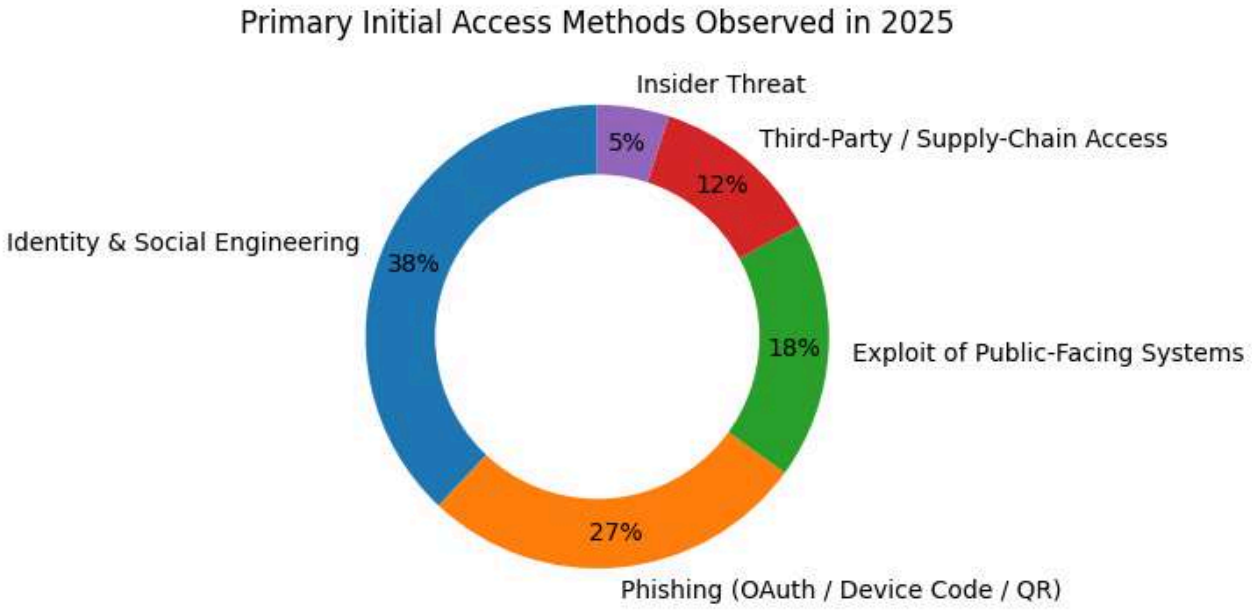
Vulnerability exploitation remained a key entry point, but attackers focused almost exclusively on High and Critical flaws, often weaponising them within days of disclosure.



Primary Initial Access Techniques Observed in 2025

The most significant shift in 2025 was how attackers gained access.

- Traditional malware delivery featured far less prominently than in previous years.
- Help desk impersonation became a highly effective technique, particularly against organisations with outsourced IT support or high staff turnover.
- OAuth and device code phishing enabled attackers to gain persistent access to Microsoft 365 and other cloud platforms without stealing passwords or bypassing MFA in a traditional sense.
- Exploited public-facing systems remained relevant, especially where patching lagged on edge devices, VPNs, and management interfaces.
- Supply-chain access was repeatedly used to pivot into multiple downstream organisations through trusted vendors, MSPs, and shared platforms.
- Insider activity, both malicious and coerced, contributed to several high impact breaches, particularly in data rich and regulated environments.



Most Frequently Targeted Technologies

Certain platforms and technologies appeared repeatedly throughout the Threat Pulse updates, reflecting where attackers found the most leverage.

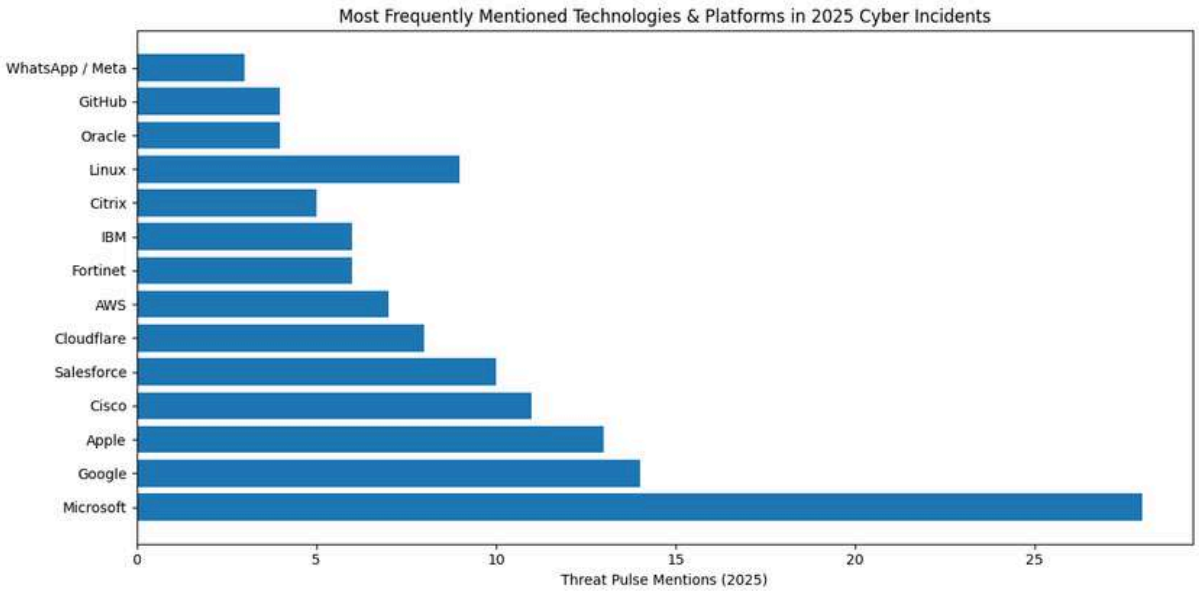
Cloud identity platforms and SaaS ecosystems were central to many incidents, as compromised tokens or misconfigurations enabled access at scale. Microsoft 365, Entra, and CRM platforms featured heavily due to their central role in business operations and collaboration.

Network edge and management systems such as VPNs, update services, and appliance management interfaces remained attractive targets when exposed or poorly segmented. Cloud infrastructure services, particularly object storage and containerised environments, were increasingly abused as attackers shifted away from endpoint-centric attacks.

Developer tooling and software supply chains appeared more frequently, with compromised repositories, extensions, and build environments used to distribute malicious code downstream.

Most referenced technologies and companies in 2025:

- Microsoft cloud and identity services
- Salesforce and CRM platforms
- Cloudflare and major internet infrastructure providers
- Fortinet, Cisco, and edge networking devices
- AWS cloud services and storage platforms
- Software development ecosystems and package repositories



Most Prevalent Attack Methods in 2025

- **Identity and help desk impersonation**

Attackers posed as employees or contractors to reset credentials or add MFA devices.

- **OAuth and device-code phishing**

Users were tricked into approving access on legitimate login pages, granting attackers persistent access without password theft.

- **Token and API key theft**

Compromised SaaS tokens and cloud credentials were reused to access multiple systems and tenants.

- **Supply-chain and SaaS compromise**

A single vendor breach was used to pivot into hundreds of downstream organisations.

- **Living-off-the-land techniques**

Native tools such as PowerShell, certutil, curl, and WMI were used instead of custom malware.

- **Exploitation of public-facing systems**

High and Critical vulnerabilities in edge devices, update services, and management interfaces were rapidly weaponised.

- **Data exfiltration before disruption**

Sensitive data was stolen first, with encryption or service disruption applied later or not at all.

- **Ransomware deployed post-access**

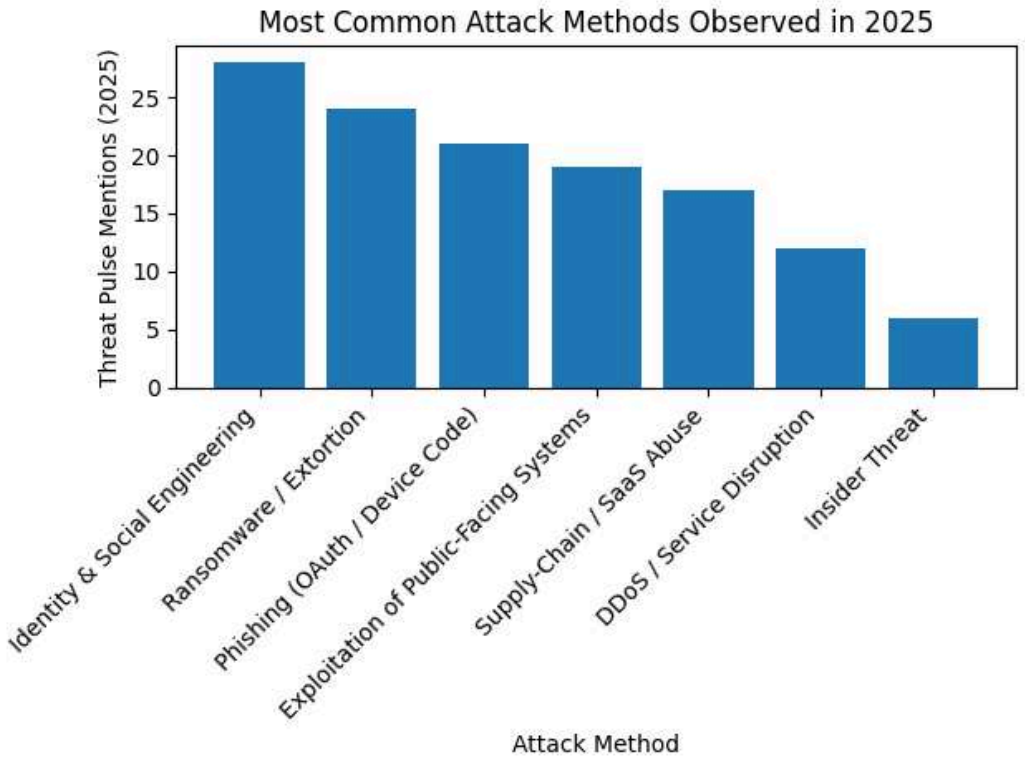
Encryption was often the final step, used only once access, persistence, and leverage were established.

- **DDoS and service disruption**

High-volume traffic attacks were used to disrupt services, amplify extortion pressure, or align with geopolitical events.

- **AI-assisted social engineering**

AI was used to craft more convincing phishing, fraud, and extortion narratives at scale.



Why These Methods Worked

- **They exploited trust rather than technology**

Identity abuse and SaaS access bypassed many traditional security controls.

- **They blended into normal activity**

Legitimate tools and platforms made malicious actions harder to distinguish from day-to-day operations.

- **They reduced detection opportunities**

Malware-free and token-based attacks often generated fewer alerts for SOC teams.

- **They scaled efficiently**

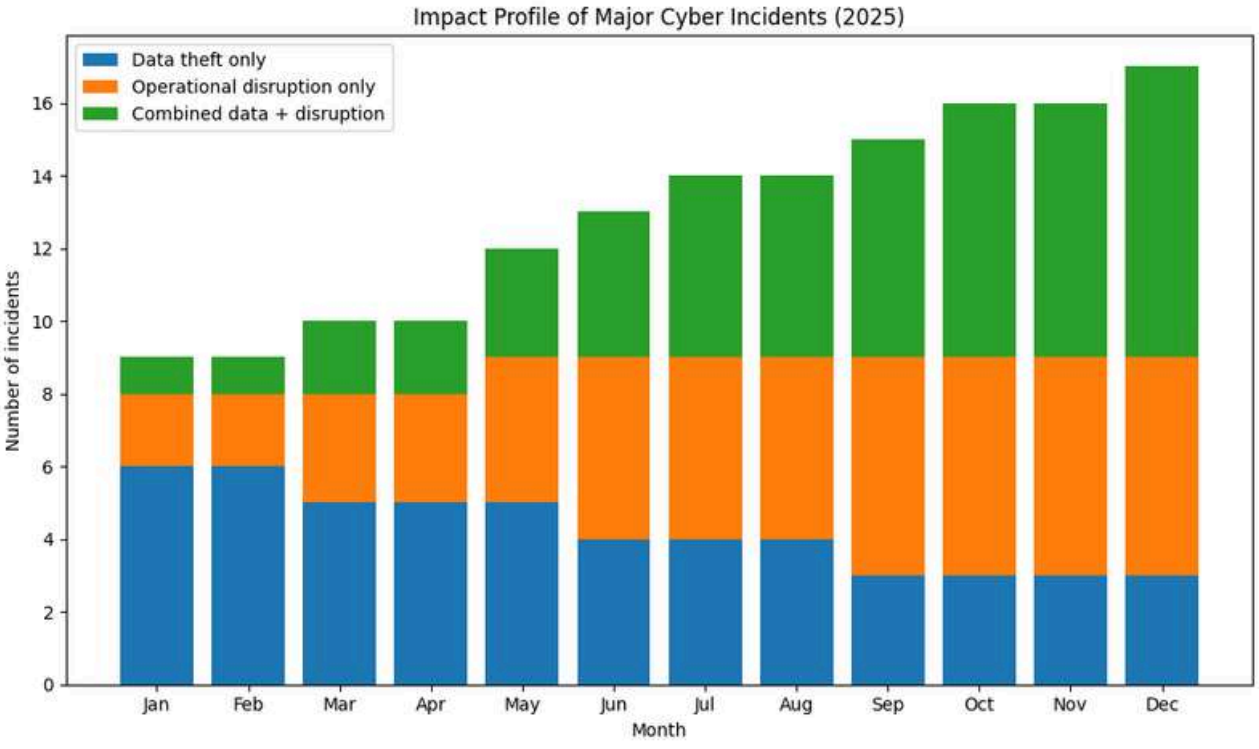
Supply-chain access and SaaS compromise allowed one intrusion to impact many victims.

- **They maximised business pressure**

Data theft and disruption targeted operations, safety, and reputation, not just IT systems.

- **They adapted faster**

Attackers weaponised vulnerabilities and social engineering techniques faster than organisations could respond to the evolving tactics.



Key Cyber Threat Trends of 2025

The 2025 threat landscape was defined less by novelty and more by convergence. Attackers refined a small number of reliable techniques and applied them repeatedly across sectors, geographies, and technologies. The result wasn't a louder year, but one marked by deeper access, wider impact, and greater operational disruption.

Several trends dominated throughout the year:

- Ransomware remained the most common threat, but encryption was no longer essential to success. Data theft, service disruption, and extortion pressure increasingly delivered the desired outcome without deploying a payload.
- Identity became the primary initial access vector. Attackers focused on people, processes, and trust relationships rather than technical vulnerabilities alone.
- Supply-chain and SaaS breaches dramatically amplified impact, allowing a single compromise to cascade across hundreds of organisations.
- Manufacturing, healthcare, retail and public sector organisations were the most consistently targeted due to operational dependency, legacy environments, and low tolerance for downtime.

Initial Access Methods

Theme: Identity became the front door.

Across the year, initial access techniques shifted decisively away from traditional malware delivery. Instead, attackers repeatedly abused identity systems and human workflows to gain legitimate looking access.

- Help desk impersonation, where attackers convinced support teams to reset credentials or enrol new authentication factors.
- OAuth and device-code phishing, which tricked users into authorising attacker-controlled applications on legitimate login pages.
- Token theft from SaaS platforms and cloud services, enabling persistent access without password compromise.
- Guest tenant abuse, particularly in collaboration platforms, where security controls were inherited from weaker external environments.
- SIM swapping, used to intercept authentication codes and reset accounts tied to mobile numbers.

These methods bypassed many traditional preventative controls and generated minimal security telemetry, making them highly effective.

Attack Methodology and Adversary Playbooks

Theme: Access → Persistence → Exfiltration → Leverage.

By mid-2025, a clear and repeatable attacker playbook had emerged. Rather than isolated actions, attacks followed a structured sequence designed to maximise leverage while minimising detection.

- Credential theft using infostealers or lightweight remote access tools to establish initial footholds.
- Persistence mechanisms such as webshells, backdoors, scheduled tasks, or rootkits to survive reboots and credential resets.
- Data exfiltration using cloud storage services or encrypted command-and-control channels that blended into normal traffic.
- Extortion pressure applied through deadlines, staged data leaks, and threats of deletion or operational disruption.

This approach allowed attackers to control timing and escalation, often engaging victims only once maximum leverage had been established.

Legitimate Infrastructure as Camouflage

Theme: Hiding in plain sight.

One of the most consistent tactics of 2025 was the abuse of trusted platforms and built-in functionality as a cover for malicious activity. Rather than introducing suspicious tools, attackers hid inside environments that organisations already relied on.

- Microsoft OAuth and Microsoft 365 domains, used for phishing, token abuse, and application consent attacks.
- SaaS platforms and APIs, which provided ready-made access paths into business-critical data.
- Signed and notarised installers on macOS, which reduced user suspicion and bypassed basic security checks.
- Browser features such as push notifications, used for fileless phishing and redirection.
- Living-off-the-land utilities including PowerShell, certutil, and curl, which blended into administrative activity.

This camouflage significantly reduced detection rates, plus it extended attacker dwell time.

Ransomware and Extortion Trends

Theme: Evolution, not explosion.

Ransomware didn't disappear in 2025, but its role changed. There were fewer genuinely new families and far more reuse, rebranding, and affiliate-driven operations. Encryption was often optional, deployed only when it added pressure.

The most significant shift was impact beyond encryption. Attackers increasingly focused on:

- Manufacturing shutdowns that halted production lines.
- Retail attacks that wreaked havoc on online and delivery services.
- Aviation and transport disruption that caused cascading delays.
- Public sector and council outages that affected citizen services and trust.

These outcomes delivered leverage even when backups were intact and systems could be restored.

Attack Methodology Strains Identified in 2025

Meta-pattern observed in 2025: attackers didn't force entry. They logged in, blended in, and waited.

The following methodology strains appeared repeatedly across the Threat Pulse updates, often in combination:

Identity-First Intrusion

How it works: Attackers gain access by abusing identity systems and support processes rather than deploying malware.

2025 indicators: Help desk impersonation, OAuth abuse, guest access exploitation, insider-assisted breaches.

Why it matters: Security tools are bypassed entirely and access appears legitimate.

Executive takeaway: If identity is compromised, perimeter controls are irrelevant.

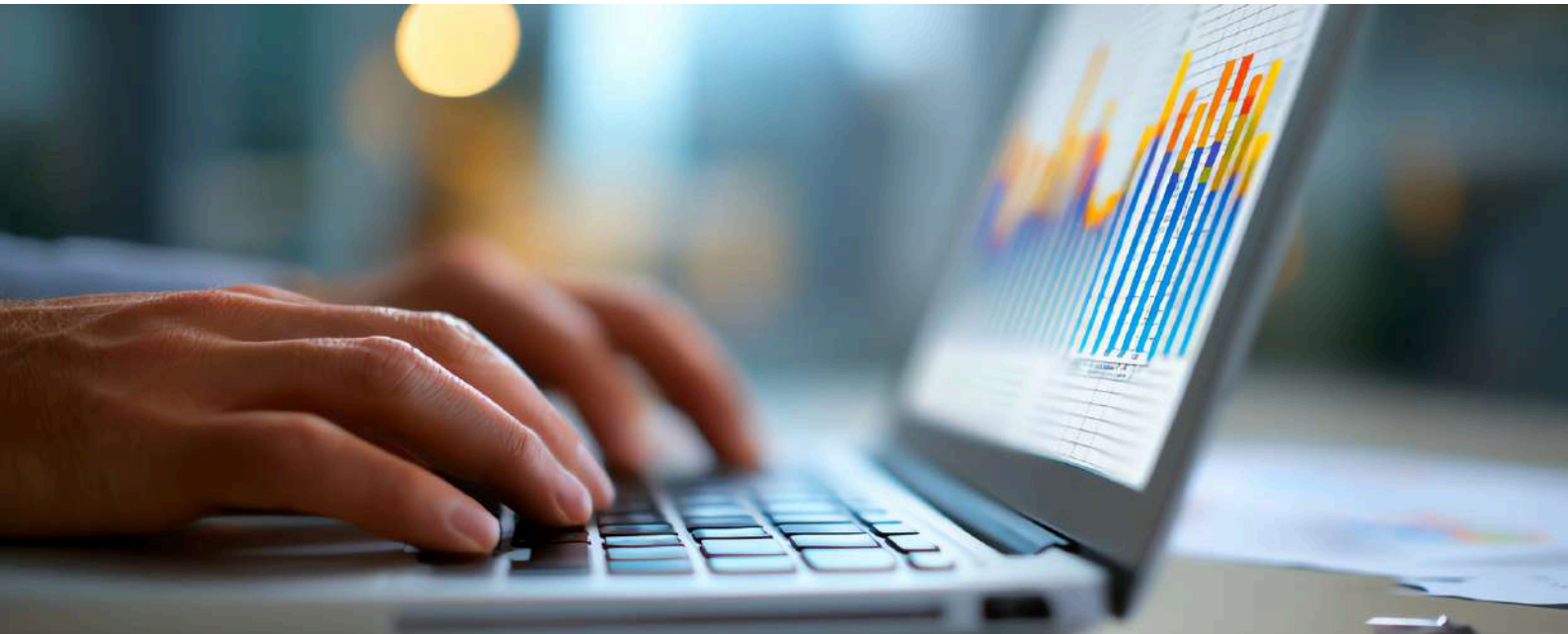
Living-Off-The-Land Persistence

How it works: Native tools and signed binaries are used to maintain access and move laterally.

2025 indicators: PowerShell-based activity, WSUS abuse, Exchange and SharePoint exploitation, fileless implants.

Why it matters: Activity blends into normal administration and evades signature-based detection.

Executive takeaway: Attackers stopped bringing tools and started using yours.



Supply-Chain and SaaS Compromise

How it works: A trusted vendor or platform is compromised and used as a bridge into customer environments.

2025 indicators: CRM token theft, MSP breaches, healthcare and council vendor incidents.

Why it matters: Impact scales rapidly beyond the initial victim.

Executive takeaway: Your biggest risk may sit outside your organisation.

Cloud Control-Plane Abuse

How it works: Attackers exploit cloud identities, APIs, and control-plane features rather than endpoints.

2025 indicators: Cloud storage extortion, token misuse, container escape vulnerabilities.

Why it matters: Detection is complex and responsibility is often unclear.

Executive takeaway: The attack surface has moved above the operating system.

Blended Multi-Stage Campaigns

How it works: Identity abuse, persistence, data theft, and disruption are combined into a single campaign.

2025 indicators: Manufacturing shutdowns, healthcare vendor attacks, retail and aviation disruption.

Why it matters: Incident response becomes cross-functional and time-critical.

Executive takeaway: Modern attacks are campaigns, not incidents.

Extortion Without Encryption

How it works: Data is stolen and leverage applied without deploying ransomware.

2025 indicators: SaaS data theft, insider-enabled exfiltration, leak-site pressure.

Why it matters: Backups don't mitigate reputational or regulatory damage.

Executive takeaway: Encryption is no longer required to extort victims.

AI-Augmented Social Engineering

How it works: AI is used to scale and personalise phishing, fraud, and extortion.

2025 indicators: Deepfake BEC, emotionally manipulative ransom demands, fake recruiters.

Why it matters: Human detection rates decline as realism increases.

Executive takeaway: Social engineering has become both scalable and convincing.

Geopolitical Hybrid Operations

How it works: State-linked actors blend espionage, disruption, and criminal tooling.

2025 indicators: Energy sector targeting, telecom espionage, hacktivist-aligned DDoS.

Why it matters: Attribution is blurred and businesses become proxy targets.

Executive takeaway: Cyber risk now mirrors geopolitical risk.

Evolving Threats Per Month

January:

- Russian and Chinese cyber espionage intensified, with multiple state-linked groups targeting government, energy, and telecoms.
- Software supply-chain attacks and cloud credential abuse emerged alongside ransomware delivered through remote assistance tools and developer-focused infostealers.

February:

- Ransomware activity surged in healthcare, with double-extortion campaigns disrupting services.
- Fake CAPTCHA pages and trojanised tooling delivered RATs, alongside insider exposure and large-scale IoT data breaches.

March:

- Ransomware campaigns hit media, healthcare, and manufacturing, often alongside AI-enhanced phishing.
- Supply-chain attacks against MSPs and ERP platforms expanded impact, while DDoS activity aligned with geopolitical tensions and transport disruption.

April:

- Help desk social engineering became a dominant access vector, particularly in UK retail.
- Chaos ransomware and corporate data extortion coincided with zero-day exploitation and large-scale forum and platform data leaks.

May:

- Play ransomware activity spiked dramatically, affecting hundreds of organisations.
- Scattered Spider targeted UK retailers, while major telecom and luxury brand data breaches and insider-assisted theft underscored the scale of identity-driven compromise.

June:

- Hacktivist-driven DDoS surged alongside growing concern around AI-powered threats and shadow AI usage.
- Telecom espionage, zero-day exploitation, and ransomware affecting healthcare and industrial environments highlighted increasing pressure on critical services.

July:

- Ransomware impacted charities and global supply chains, while aviation and transport sectors faced targeted disruption.
- A Microsoft SharePoint zero-day and hyper-volumetric DDoS attacks demonstrated how quickly new vulnerabilities were weaponised.

August:

- Mega-breaches in telecoms and credit reporting exposed millions of records.
- Salesforce-driven supply-chain attacks, manufacturing espionage, and deepfake-enabled fraud showed attackers combining scale with precision.

September:

- Ransomware caused severe industrial disruption, including prolonged manufacturing outages.
- Supplier breaches shut down aviation systems, while SaaS token theft and zero-day exploitation accelerated across finance and real estate.

October:

- Active exploitation of enterprise infrastructure such as WSUS, Exchange, and network devices increased.
- OAuth abuse, developer ecosystem supply-chain attacks, and malware-free intrusion techniques reflected rising sophistication and stealth.

November:

- Zero-day exploitation occurred at scale, including kernel and application-layer flaws.
- Cloud and internet infrastructure outages, SaaS token abuse, and public sector incidents highlighted systemic and shared-service risk.

December:

- OAuth device-code phishing and VPN edge device exploitation dominated initial access.
- macOS infostealers abusing signed applications, emergency zero-day patching, healthcare supplier breaches, and renewed manufacturing ransomware closed the year with sustained pressure..

Key Observations & Emerging Threat Trends

Looking at the strongest patterns observed across the 2025 Threat Pulse updates, we can see how attacker behaviour changed over the year, why those changes matter, and what they signal for organisational risk going forward

Threat Type Dominance Over Time

Observed patterns:

- Ransomware and extortion activity appeared in every single month of 2025
- Early-year campaigns focused more heavily on encryption
- Mid to late 2025 saw a clear shift toward data theft, disruption, or both
- Many incidents caused material damage without deploying encryption at all

Why it matters

Ransomware is no longer a purely technical problem. Even when encryption is avoided or interrupted, attackers still achieve leverage through stolen data, service outages, or operational paralysis. This shifts the problem firmly into business continuity, crisis management, and reputational risk rather than IT recovery alone.

Executive takeaway

Ransomware didn't disappear in 2025, but its purpose changed from locking files to stopping organisations from operating.

Initial Access Methods: Identity Beats Exploits

Observed patterns:

- Identity-based entry points recur throughout the year
- Help desk impersonation and MFA fatigue attacks became routine
- OAuth and device-code phishing appeared repeatedly across SaaS and cloud platforms
- Token theft and guest tenant abuse enabled access without malware

Why it matters

These attacks bypass traditional perimeter and endpoint controls entirely. They succeed not because security tooling fails, but because trust is exploited. Once identity is compromised, access appears legitimate and is difficult for SOC teams to distinguish from normal activity.

Executive takeaway

In 2025, the primary control point attackers targeted was identity, not infrastructure. Organisations that focused security investment on perimeter and endpoint controls without equivalent rigour around identity governance, help desk processes, and SaaS access created a structural blind spot that attackers repeatedly exploited.

Sector Targeting

Observed patterns:

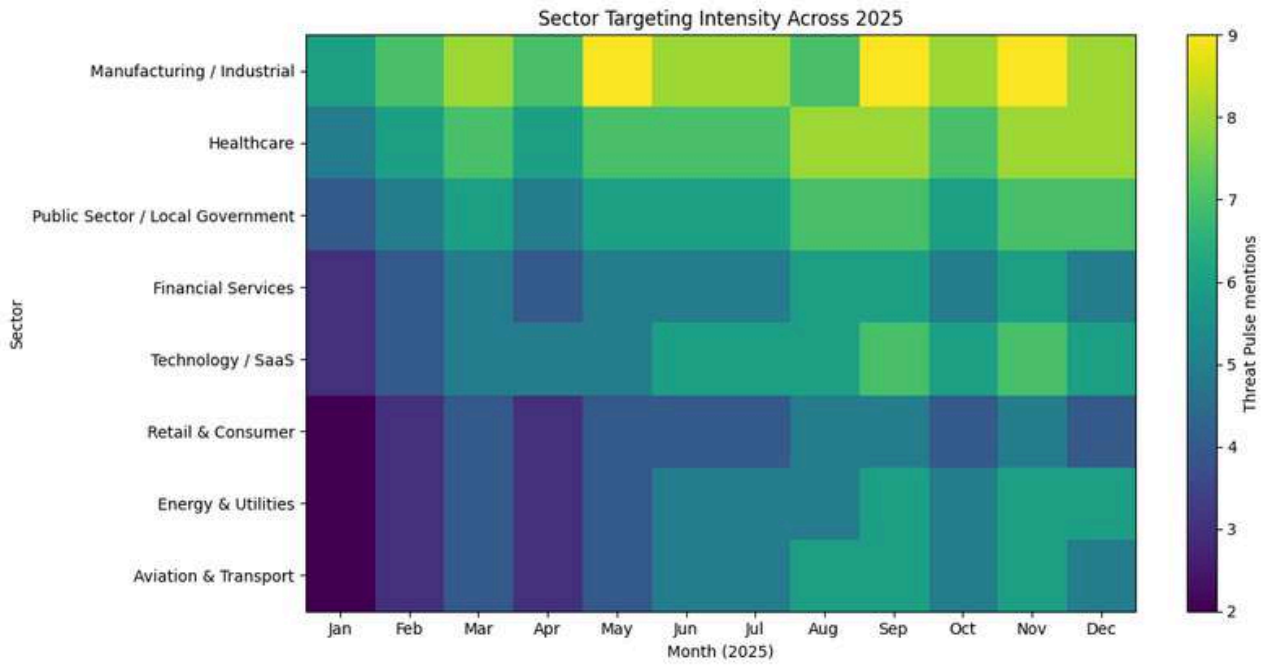
- Manufacturing, healthcare, retail and public sector organisations dominate month after month
- Attacks frequently intersect with OT, legacy systems, and supplier dependency
- These sectors experienced repeat targeting rather than isolated spikes

Why it matters

These environments combine high operational impact with low tolerance for downtime. Disruption creates immediate leverage, whether financial, political, or strategic. This makes them ideal targets for extortion, espionage, and sabotage.

Executive takeaway

Attackers consistently targeted sectors where disruption creates immediate operational, safety, or societal pressure. For organisations in manufacturing, healthcare, retail, and the public sector, cyber risk is inseparable from operational resilience and continuity planning, not just data protection.



Supply-Chain and SaaS Blast Radius Effect

Observed patterns:

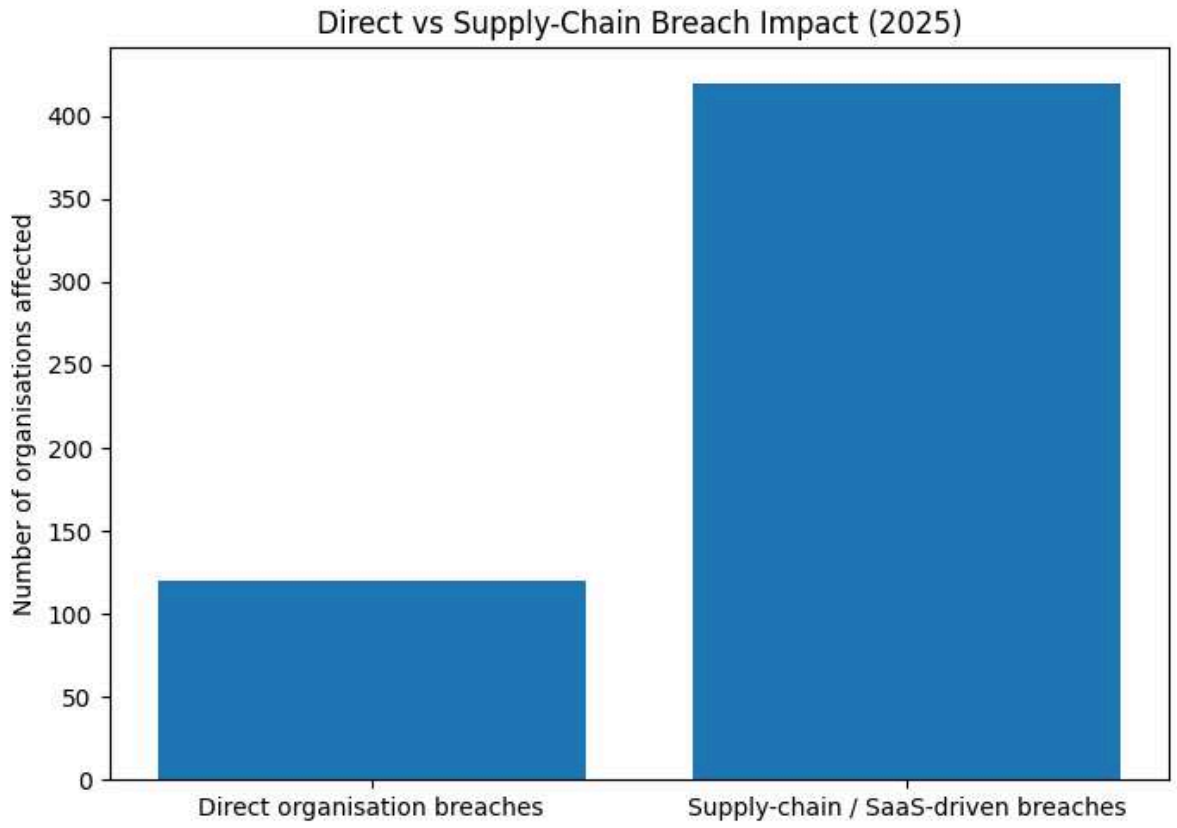
- Many of the largest incidents originated in SaaS platforms, MSPs, or vendors
- Single breaches cascaded into hundreds of downstream victims
- Token reuse and trusted integrations enabled rapid lateral spread

Why it matters

Cyber risk increasingly exists outside organisational boundaries. A company can do everything right internally and still be compromised through a trusted third party. This reframes cyber security as an ecosystem risk, not an internal one.

Executive takeaway

In 2025, the scale of impact was determined less by the victim organisation and more by its position in a digital ecosystem. Organisations that rely heavily on SaaS platforms, managed service providers, and shared services inherited risk from those partners, making third-party governance and visibility a board-level concern rather than a procurement exercise.



CVE Severity Distribution

Categorisation of CVEs:

- 100 percent of CVEs referenced were rated High or Critical
- Nearly half fell into the Critical category
- No medium or low severity vulnerabilities featured in major incidents

Observed patterns:

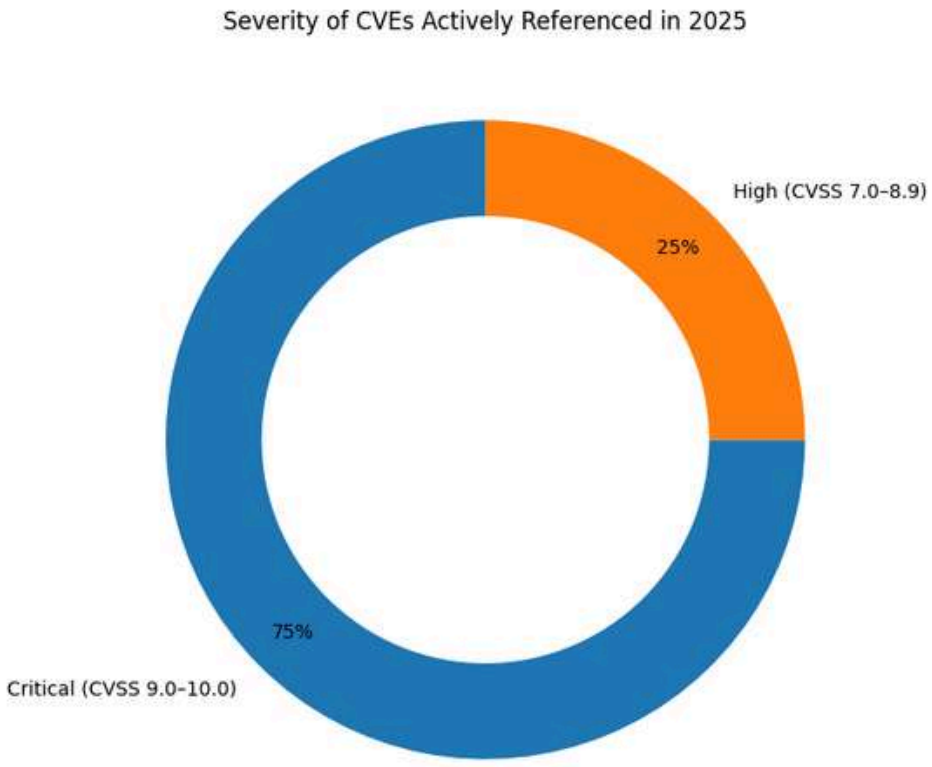
- Exploitation frequently followed disclosure within days or hours
- Edge devices, identity platforms, and update mechanisms were favoured
- CVEs were often used to accelerate access rather than form full attack chains

2024 pattern versus 2025 evolution

In 2024, high-severity vulnerabilities were exploited, but often with a longer delay. In 2025, speed became the differentiator. Patch latency, not vulnerability volume, emerged as the dominant risk factor.

Executive takeaway

In 2025, attackers ignored low-severity vulnerabilities to make a bigger and longer lasting impact.



DDoS and Disruption as a Strategic Tool DDoS and Disruption as a Strategic Tool

Observed patterns

- Hacktivist-driven DDoS surges aligned with geopolitical events
- Platform and vendor outages created widespread collateral disruption
- Livestreams, public events, and high-visibility services were targeted

Why it matters

DDoS is no longer just noise or extortion cover. It's increasingly used as a political and strategic pressure tool, designed to disrupt public confidence, operations, and visibility.

Executive takeaway

In 2025, denial-of-service activity evolved into a strategic disruption tool rather than a technical nuisance. Organisations should treat large-scale DDoS and platform disruption as a business continuity and reputational risk, particularly where services are public-facing, time-sensitive, or symbolically significant.

Operational Disruption vs Data Theft

Observed patterns

- Manufacturing shutdowns caused prolonged production losses
- Aviation and transport systems experienced service delays
- Councils and public services suffered outages affecting citizens
- Data theft increasingly coincided with, or was replaced by, disruption as seen in retail sector attacks

Why it matters

Availability is now as valuable to attackers as confidentiality. Cyber incidents increasingly translate directly into lost revenue, safety risks, and public trust erosion.

Executive takeaway

Operational availability emerged as a primary leverage point for attackers in 2025. Boards should treat cyber incidents as potential operational crises, not just information security issues, and ensure that resilience, recovery, and decision-making under disruption are actively planned and rehearsed.

Criminal vs State-Linked Activity

Observed patterns

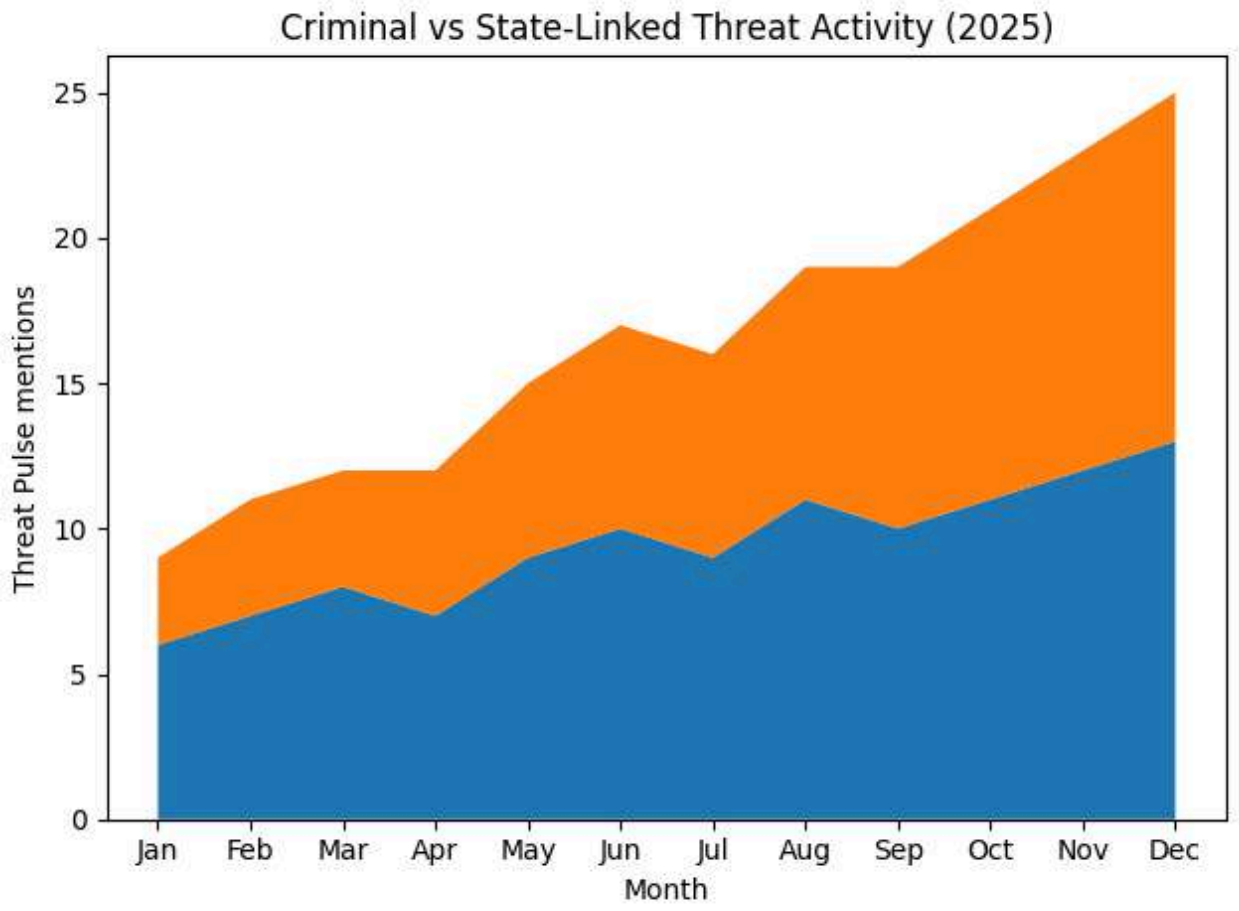
- Criminal and state-linked activity increased in parallel
- Tools and infrastructure overlapped significantly
- Attribution became deliberately blurred

Why it matters

The boundary between cybercrime and geopolitics continues to erode. Businesses are increasingly caught as proxy targets in wider strategic conflicts, even when they are not the intended end goal.

Executive takeaway

The increasing overlap between criminal and state-linked activity means organisations can no longer rely on simple threat categorisation. Cyber risk management must assume hybrid actors, ambiguous attribution, and attacks that serve both financial and geopolitical objectives, even when the immediate impact appears commercially motivated.



Attack Complexity Curve

Observed patterns

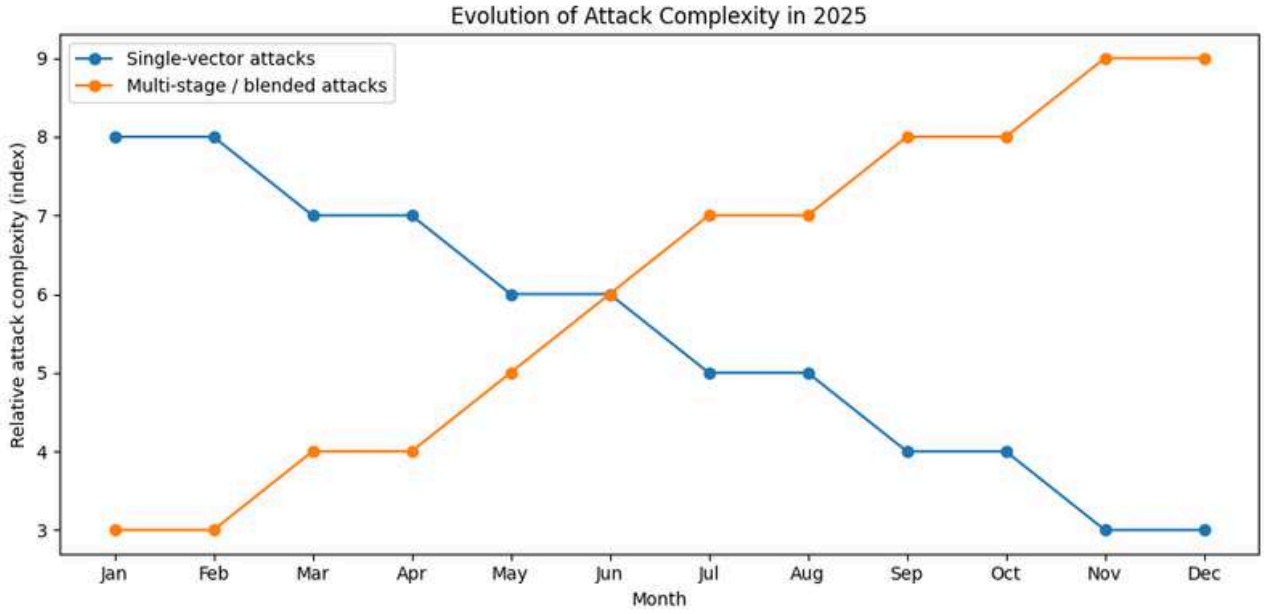
- Early 2025 incidents were often single-vector and noisy
- Later campaigns blended identity abuse, living-off-the-land techniques, and extortion
- Malware-free intrusions became more common

Why it matters

Traditional SOC models struggle when attacks look like normal administrative activity. Detection becomes harder, dwell time increases, and containment requires deeper context across identity, cloud, and endpoints.

Executive takeaway

By the second half of 2025, many successful intrusions no longer resembled traditional cyberattacks. They resembled legitimate administrative activity. This shift demands a rethink of SOC effectiveness, with greater emphasis on identity telemetry, behavioural context, and cross-platform visibility rather than reliance on malware detection alone.



Geopolitical Overlay

Observed patterns

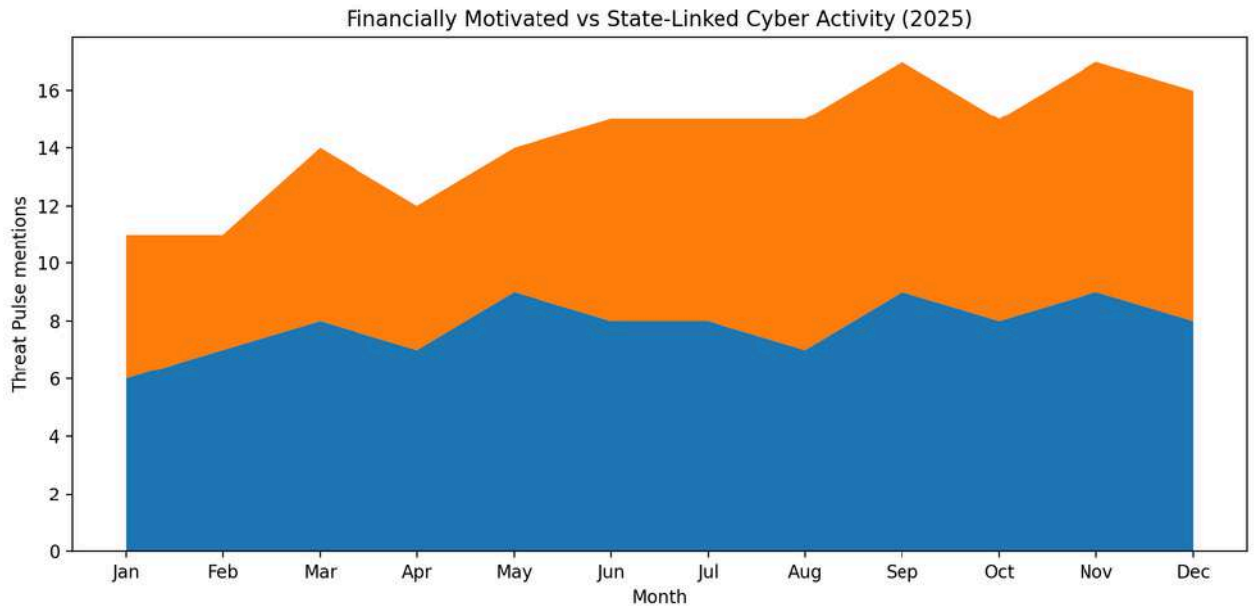
- State-linked APT activity persisted throughout the year
- DDoS spikes correlated with geopolitical tension
- Energy, telecoms, and government entities remained consistent targets

Why it matters

Cyber risk can no longer be separated from geopolitical context. Organisations may be targeted not for who they are, but for what they represent or support.

Executive takeaway

Cyber threats in 2025 increasingly reflected geopolitical tension rather than purely criminal intent. Organisations should recognise that sector, geography, and strategic relevance can elevate their risk profile, even in the absence of direct targeting, and factor geopolitical exposure into cyber risk assessments and scenario planning.



Ransomware Evolution

Ransomware in 2025 didn't disappear, but it fundamentally changed character.

Encryption became optional rather than essential. Attackers increasingly focused on gaining access, extracting data, disrupting operations, and applying pressure where it hurt most.

In many cases, the threat of exposure or service outage proved just as effective as locking files. This extortion-first approach reduced attacker risk, shortened attack timelines, and complicated defensive response, particularly where incidents straddled legal, regulatory, and operational boundaries.

New Ransomware Strains of 2025

Codefinger

- Features: Targets cloud-native environments, particularly AWS S3 buckets. Uses server-side encryption with customer-provided keys to lock data without deploying endpoint malware. Relies on compromised cloud credentials rather than traditional infection vectors.
- Impact: Bypasses endpoint security and EDR controls entirely. Poses significant risk to SaaS providers and software vendors. Demonstrates ransomware shifting into the cloud control plane.

Hyena

- Features: Focuses on utilities and CNI. Exploits unpatched Windows systems and OT-adjacent assets. Prioritises rapid encryption of operational data.
- Impact: High risk of service outages and safety disruption. Reinforces the appeal of environments with low downtime tolerance.

Datarip

- Features: Enhanced evasion capabilities. Harvests credentials before deploying any ransomware payload. Delays encryption to extend dwell time.
- Impact: Blurs the line between ransomware and infostealer campaigns. Makes early detection significantly harder for SOC teams.

NightSpire

- Features: Double extortion ransomware with large-scale data exfiltration. Targets manufacturing and industrial. Uses stealthy lateral movement before encryption.
- Impact: Theft of intellectual property, blueprints, and proprietary processes. Creates long-term competitive and supply-chain risk beyond ransom payment.

RansomHub

- Features: Operates as a Ransomware-as-a-Service platform. Targets mid-sized companies across multiple sectors. Combines data theft, encryption, and leak-site pressure.
- Impact: Low barrier to entry increases attack volume. Accelerates the industrialisation of ransomware operations.

Interlock

- Features: Targets healthcare and life sciences environments. Steals large volumes of regulated data before encryption. Emphasises regulatory and reputational pressure.
- Impact: Exposure of sensitive patient and clinical data. Forces victims into complex legal and compliance crises.

SafePay

- Features: Targets healthcare and life sciences environments. Steals large volumes of regulated data before encryption. Emphasises regulatory and reputational pressure.
- Impact: Targets technology distributors and supply-chains. Deploys attacks during holidays or low-staffing periods. Focuses on maximum downstream disruption.

Chaos (modern variant)

- Features: Often deployed following help desk impersonation or identity abuse. Used as a post-access monetisation step rather than initial entry. Lightweight and fast-moving encryption routines.
- Impact: Reinforces identity compromise as the true root cause. Ransomware becomes the final step, not the beginning.

Ransomware Strains in 2025

Alongside the newer and evolved families, 2025 also saw continued activity from established groups such as Play, Medusa, Qilin, Rhysida, LockBit affiliates, Akira, and SafePay-linked operators.

Rather than a surge in entirely new families, the year was defined by reuse, rebranding, and affiliate-driven operations.

Key Ransomware Trends in 2025

- Data theft became the primary leverage mechanism, with encryption often delayed or avoided
- Ransomware-as-a-Service platforms lowered the barrier to entry and increased attack volume
- Attacks were frequently timed around holidays, weekends, or known low-resourcing periods
- Pressure tactics became sector-specific, exploiting safety, regulatory, or operational concerns
- Disruption and downtime increasingly replaced file encryption as the monetisation goal

Impact of Ransomware in 2025

Operational impact

- Manufacturing shutdowns halted production for days or weeks
- Aviation and transport systems experienced delays and cancellations
- Councils and public services faced prolonged service outages

Regulatory and reputational impact

- Data exposure triggered mandatory breach notifications and regulatory scrutiny
- Victims faced reputational damage even where encryption was avoided
- Incident recovery increasingly involved legal, communications, and executive leadership

Strategic Recommendations for Ransomware Defence

- Treat identity security as a core ransomware control, not a separate discipline
- Harden help desk processes and verify all privileged access requests
- Implement continuous monitoring for data exfiltration and abnormal cloud activity
- Test incident response and crisis management plans, not just backups
- Review supplier and SaaS risk with the same scrutiny as internal systems
- Prepare for extortion scenarios that don't involve encryption
- Align ransomware defence with business continuity and operational resilience planning

Ransomware in 2025 proved that prevention alone isn't enough. Resilience, visibility, and readiness now define effective defence.

AI Cyber Threats in 2025

Artificial intelligence became a force multiplier for attackers in 2025. Rather than introducing entirely new categories of crime, AI was used to scale, personalise, and accelerate existing techniques.

Phishing campaigns became more convincing and harder to spot, with language models generating fluent, context-aware messages tailored to specific roles, organisations, and ongoing events. Device-code phishing, OAuth consent abuse, and fake support interactions benefited directly from AI-generated content that removed the tell-tale signs users were trained to recognise.

Deepfakes moved from proof of concept to operational use. Voice cloning and synthetic video were used in business email compromise and executive fraud, particularly in financial and professional services sector targeting. These attacks were often short, targeted, and timed to coincide with periods of urgency, such as quarter-end payments or executive travel.

AI also played a role in reconnaissance and targeting. Threat actors used automation to analyse breached datasets, public profiles, and organisational structures to identify high value users, privileged roles, and likely trust paths. This reduced manual effort and increased success rates, particularly in identity led intrusions.

On the tooling side, AI-assisted malware and ransomware development became more visible. While most ransomware families were evolutions rather than brand new codebases, AI was used to accelerate scripting, obfuscation, configuration generation, and even ransom note customisation.

This lowered the barrier to entry for affiliates and enabled faster iteration of payloads and evasion techniques.

Impact of AI on Cyber Security in 2025

The widespread use of AI by attackers exposed the limits of traditional security awareness and control models.

Many defences are built on recognising known patterns, suspicious language, or abnormal behaviour. AI-generated content deliberately avoids these signals, producing communications that appear routine, polite, and plausible.

Users trained to look for spelling errors, generic greetings, or poor grammar were confronted with highly polished messages that referenced real projects, colleagues, or suppliers. In parallel, MFA and email security controls were bypassed through OAuth abuse and token theft, meaning successful attacks often involved no malware and no obvious indicators.

Executive targeting intensified as a result. Deepfake voice calls, AI-written payment requests, and highly tailored phishing emails increased both the speed and scale of fraud.

Attackers no longer needed prolonged access to succeed. A single convincing interaction could trigger six-figure losses or grant access to sensitive systems.
For defenders, AI did contribute to an increase in automated attack activity and a higher volume of low-signal events that blended into normal operations, particularly across cloud and identity platforms.

However, organisations supported by mature SOC capabilities were able to counter this shift by applying AI-driven detection, threat-led use cases, advanced behavioural analytics, and expert-led tuning, to separate meaningful threat activity from background noise.

This reinforced a clear distinction in 2025 between reactive monitoring and intelligence-led SOC operations, where scale and automation could be met with equally advanced defensive capability.

AI-Enabled Cybercrime Trends to Watch in 2026

Looking ahead, several AI-driven trends are likely to shape the threat landscape in 2026.

Agentic AI represents a significant risk. These systems can plan, execute, and adapt attack steps with minimal human input. In a cyber context, this could mean autonomous reconnaissance, dynamic phishing campaigns, or automated lateral movement based on live feedback from target environments.

Even limited adoption could significantly increase attack speed and dwell time.

Deepfake-enabled fraud is expected to mature further. As voice and video synthesis improves, verification based on familiarity or recognition will become unreliable.

Attackers will increasingly target executives, finance teams, and help desks using synthetic identities that closely mimic trusted individuals.

Emotional manipulation at scale, sometimes referred to as vibe-hacking, is another emerging concern.

AI systems are already being used to craft messages designed to elicit urgency, fear, trust, or sympathy.

In 2026, these techniques are likely to be combined with real-time context and behavioural data, making scams more persuasive and harder to resist.

Taken together, these trends suggest that AI will continue to fuel attackers who exploit trust, identity, and human decision-making.

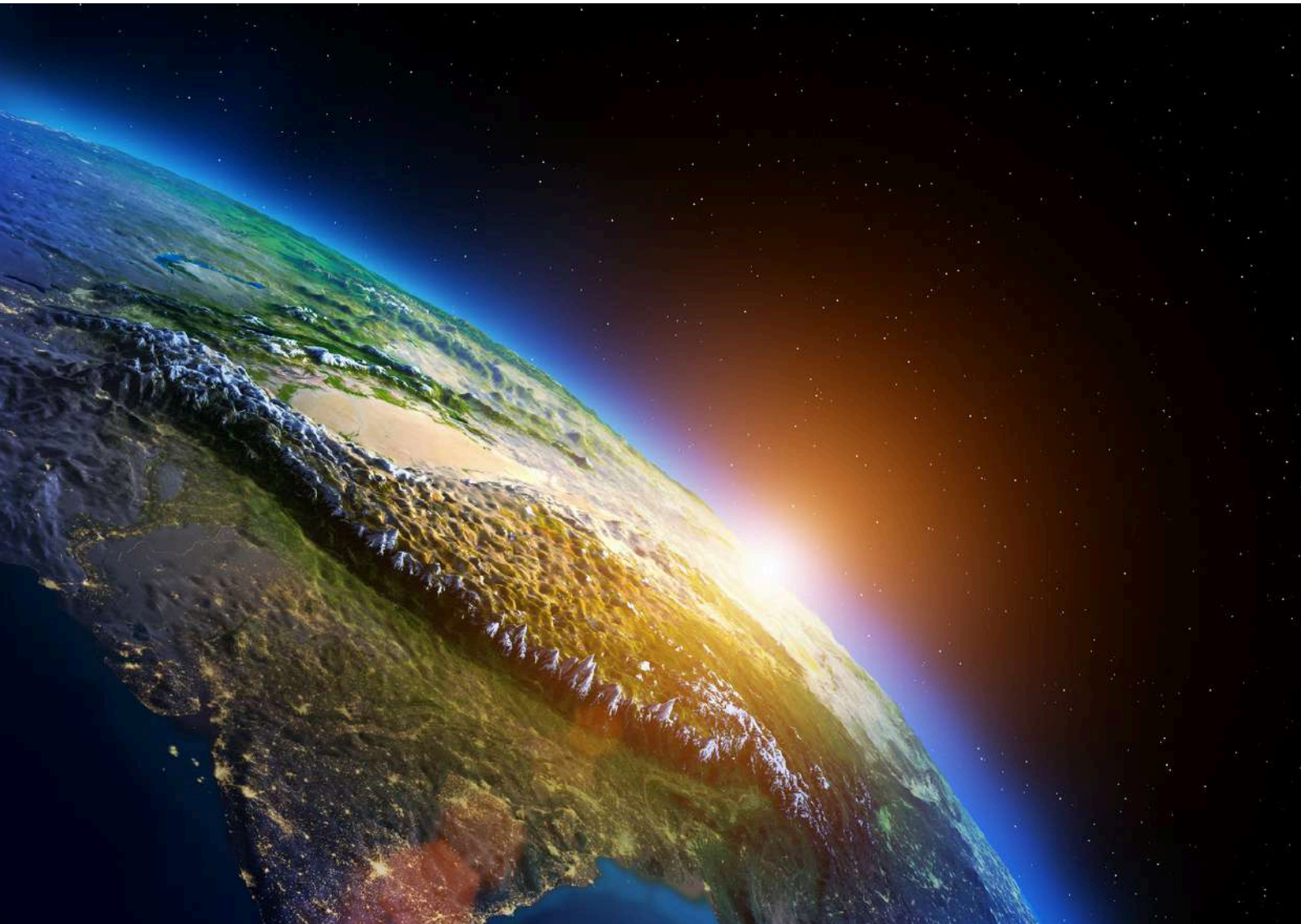
Defending against AI-enabled threats will require next-gen advanced capabilities, stronger identity controls, better verification processes, and a shift away from reliance on user judgement alone.

Targeted Sectors and Geographical Focus

Throughout 2025, threat activity consistently concentrated on sectors where downtime is costly, safety is critical, and recovery is complex.

Rather than spreading attacks evenly across the economy, adversaries repeatedly focused on environments where operational impact creates leverage, whether financial, political, or strategic.

This targeting reflects a clear understanding of how modern organisations operate, where dependencies exist, and which sectors are least able to tolerate interruption.



Most Targeted Sectors in 2024

Manufacturing and Industrial

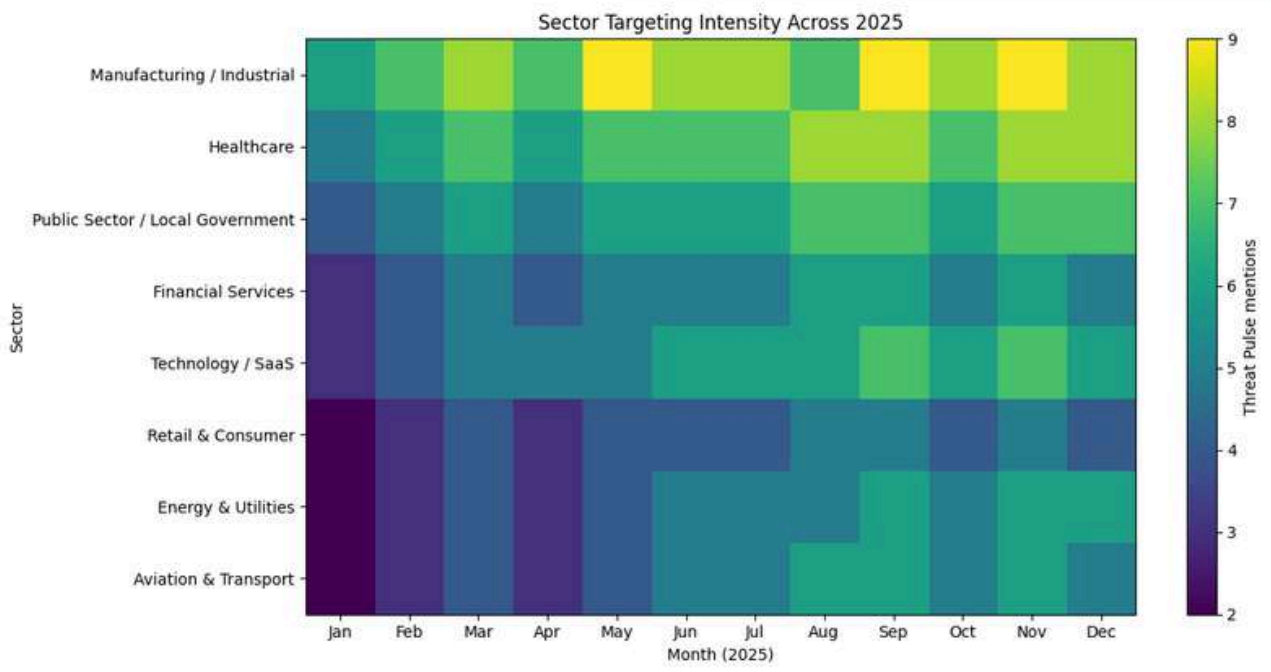
Manufacturing and industrial organisations were among the most persistently targeted sectors across the year. Attacks frequently focused on environments where IT and operational technology intersect, including production systems, supply chain platforms, and industrial control networks.

Ransomware, data theft, and extortion campaigns repeatedly caused production shutdowns, delayed deliveries, and long recovery periods. For attackers, manufacturing offers high leverage because downtime directly affects revenue, contractual obligations, and safety.

Healthcare

Healthcare remained a high-risk sector throughout 2025. Hospitals, clinics, and healthcare vendors were targeted not only because of the sensitivity of patient data, but because service disruption can have immediate real-world consequences.

Attackers increasingly focused on third-party suppliers such as pathology labs, software providers, and billing platforms, amplifying the impact across multiple organisations at once. Regulatory pressure and public trust concerns further increased the leverage available to extortion-focused groups.



Public Sector

Public sector and local government organisations featured prominently in Threat Pulse updates across the year. Councils, government departments, and public agencies were affected by ransomware, data breaches, and service outages.

These environments often rely on shared services, legacy systems, and constrained budgets, making them attractive targets. Disruption to public services also creates visible impact, increasing pressure to restore operations quickly.

Retail

Retail organisations emerged as a high-impact target sector in 2025, particularly for identity-led intrusion and extortion campaigns.

Attackers frequently exploited customer-facing systems, help desks, and third-party service providers to gain initial access, before shifting focus toward operational disruption rather than large-scale data theft.

Point-of-sale systems, logistics platforms, and e-commerce operations were attractive targets due to the immediate commercial impact of downtime. Thin margins, high transaction volumes, and peak trading dependencies meant that even short disruptions resulted in lost revenue, supply chain delays, and reputational harm.

These factors reinforced retail as a sector where availability and customer trust provide significant leverage for attackers.

Financial Services

Financial services continued to face a steady volume of attacks, particularly data theft, fraud, and identity-led intrusions.

While many large institutions have mature security controls, attackers increasingly exploited third-party providers, SaaS platforms, and insider access to bypass defences.

The exposure of personal and financial data remained a key driver, alongside the potential for downstream fraud and regulatory consequences.

Technology & SaaS

Technology and SaaS providers were targeted both directly and indirectly. In many cases, the primary objective wasn't the provider itself, but its customers.

Attacks against cloud platforms, CRM systems, software vendors, and managed service providers created significant blast-radius effects, allowing attackers to access hundreds of downstream organisations through a single compromise.

Energy & Utilities

Energy and utilities experienced sustained attention from both criminal and state-linked actors.

These attacks often aligned with broader geopolitical tensions and focused on reconnaissance, persistence, and potential disruption rather than immediate monetisation.

The combination of critical infrastructure, legacy technology, and national importance makes this sector particularly sensitive to cyber activity.

Regulation, Policy & National Cyber Posture

Throughout 2025, cyber security moved further out of the technical domain and into the regulatory and national resilience spotlight. Governments, regulators, and security authorities increasingly framed cyber risk as a matter of public safety, economic stability, and national security rather than purely an IT concern.

In the UK and across the EU, the year was marked by stronger guidance, clearer expectations, and the steady expansion of regulatory accountability beyond traditional critical infrastructure operators to include suppliers, managed service providers, and software vendors. The direction of travel was clear: organisations are now expected not only to defend themselves, but to understand and manage the cyber risk they introduce to others.

UK & EU Regulatory & Policy Developments in 2025

The UK National Cyber Security Centre (NCSC) issued repeated warnings throughout the year, highlighting a sharp rise in nationally significant incidents and stressing that critical national infrastructure and its supply chain were under sustained pressure. These warnings increasingly focused on identity abuse, supplier compromise, and operational disruption rather than isolated malware incidents.

Updates to the Cyber Assessment Framework (CAF) reflected this shift. The revised guidance placed greater emphasis on resilience, recovery, and third-party dependency management, signalling that cyber maturity is now measured as much by response capability as by preventative controls.

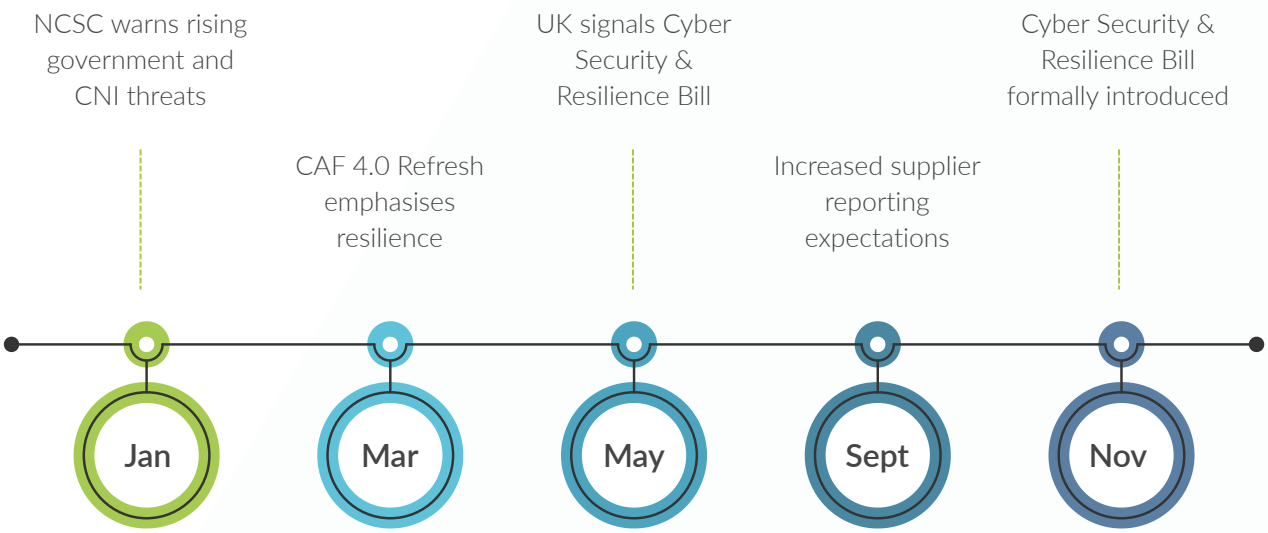
The UK Cyber Security and Resilience Bill emerged as a defining policy development. Announced, refined, and formally introduced during 2025, the bill expands regulatory oversight to a wider range of essential services and the technology providers that support them. For the first time, many suppliers and managed service providers face explicit duty-of-care obligations, mandatory incident reporting expectations, and the prospect of enforcement action for systemic weaknesses.

At EU level, the Cyber Resilience Act continued to advance, reinforcing baseline security requirements for digital products and software placed on the European market. The Act underlines a growing expectation that security must be designed into products and services from the outset, rather than added later as an operational control.

The Digital Operational Resilience Act (DORA) imposed more stringent expectations on financial services and their technology providers, with a focus on operational resilience, third-party risk, and incident testing. NIS2 further expanded the scope of regulated entities across critical and important sectors, strengthening governance requirements and enforcement powers.

Across both UK and EU frameworks, supplier scrutiny became a recurring theme. Organisations were increasingly expected to understand who they depend on, what data and access those suppliers hold, and how quickly incidents can be detected, reported, and contained across organisational boundaries.

These developments signal a fundamental change in the focus on national cyber posture. Cyber security is no longer assessed in isolation. It's evaluated through the lens of ecosystem risk, systemic resilience, and the potential for single failures to cascade across sectors.



Year-on-Year Analysis: 2024 vs 2025

Looking back across the last two years of Threat Pulse reporting, the contrast between 2024 and 2025 is clear.

While many of the same threat categories persisted, the way attackers operated, prioritised targets, and generated impact evolved significantly.

Threat Evolution: Scale vs Leverage

In 2024, cyber threats were largely characterised by scale. Attackers focused on volume, launching widespread campaigns designed to reach as many victims as possible. This period saw a steady stream of new ransomware families, commodity malware variants, and opportunistic attacks that relied on speed and breadth rather than precision. Success was often measured by how many organisations could be compromised quickly, even if individual impact varied.

2025 marked a move towards leverage. Attackers became more selective, investing time in gaining durable access, understanding their targets, and maximising business impact. Rather than flooding the landscape with new tooling, many groups reused existing malware, rebranded ransomware strains, or relied on access brokers and affiliates. The goal shifted from mass infection to sustained disruption, extortion, and strategic pressure, particularly in sectors where downtime or data exposure carried significant consequences.

Initial Access Evolution

Initial access techniques highlight one of the most important changes between the two years.

In 2024, phishing and exploitation dominated. Email-based lures, malicious attachments, and browser exploits were common entry points, often paired with newly disclosed vulnerabilities. While these techniques were effective, they also generated noise and were increasingly well understood by defenders.

In 2025, attackers moved up the stack. Help desk impersonation, OAuth abuse, token theft, and guest access exploitation became the most repeatable and reliable access paths. Rather than defeating security controls, attackers bypassed them by abusing trust, identity workflows, and legitimate access mechanisms.

This reduced reliance on malware delivery and significantly lowered the chance of early detection.

Ransomware Strategy Shift

In 2024, encryption was central. Most ransomware campaigns focused on encrypting systems as quickly as possible, then demanding payment for recovery. Data theft was present, but often secondary to the primary goal of locking systems.

In 2025, encryption became optional. Many campaigns prioritised data theft, operational disruption, or both, sometimes without deploying encryption at all.

Attackers recognised that stolen data, regulatory exposure, and service outages could deliver sufficient leverage on their own. In manufacturing, aviation, retail, healthcare, and the public sector, disruption to operations often proved more damaging than encrypted files.

Comparative Table:
2024 vs 2025 Threat Tactics

Dimension	2024 Threat Landscape	2025 Threat Landscape
Attacker objective	High-volume compromise and rapid monetisation	Maximum leverage through disruption, access, and pressure
Overall approach	Broad, opportunistic campaigns	Targeted, patient, impact-driven campaigns
Ransomware strategy	Encrypt systems to force payment	Data theft, disruption, and extortion often without encryption
Malware usage	Heavy reliance on custom malware and new ransomware strains	Reduced malware use, more reuse, rebranding, and affiliate tooling
Initial access methods	Phishing emails, malicious attachments, exploit delivery	Help desk impersonation, OAuth abuse, token theft, guest access
Identity abuse	Present but secondary	Primary and most reliable access vector
Vulnerability exploitation	Important but often chained with malware	Used selectively as access amplifiers, not full attack chains
Time to impact	Fast execution, short dwell time	Longer dwell time, delayed monetisation
Persistence techniques	Backdoors and scheduled tasks	Living-off-the-land tools, legitimate admin features, cloud roles
Detection visibility	Higher noise, easier signature detection	Low noise, legitimate activity blends into normal operations
Supply-chain risk	Present but episodic	Central attack vector with large blast-radius effects
Operational disruption	Side-effect of attacks	Explicit attacker objective
Sector targeting	Broad, cross-sector	Focused on manufacturing, healthcare, retail, public sector
Geopolitical influence	Limited to specific APT campaigns	Integrated into criminal and hybrid operations
Defender challenge	Blocking malware and patching fast	Securing identity, access, and trust relationships

What UK Organisations Should Do in 2026

The threat patterns observed throughout 2025 point to a clear conclusion: Many successful attacks didn't rely on novel malware or complex exploits, they succeeded because organisations were unprepared for identity abuse, supplier compromise, and operational disruption.

In 2026, resilience will be determined by how well controls align to real attacker behaviour, not by how many tools an organisation operates.

The priorities below are mapped directly to the dominant threat patterns seen across the Threat Pulse updates in 2025.

2026 Priority Controls

Identity-first security

- Implement strong MFA, conditional access, and strict token governance across cloud and SaaS platforms.
- Identity abuse was the most consistent initial access method in 2025, and attackers repeatedly bypassed perimeter controls by abusing legitimate accounts.

Help desk verification hardening

- Strengthen identity verification for service desks through call-back procedures, manager approval, and behavioural checks.
- Help desk impersonation featured prominently in high impact retail, aviation, and insurance incidents and remains a low cost, high return attack vector.

SaaS and third-party risk management

- Inventory SaaS usage, enforce least privilege access, and continuously assess suppliers.
- Supply chain and SaaS compromises created the largest blast radius incidents of 2025, often affecting hundreds of downstream organisations.

Continuous vulnerability exposure management

- Move beyond periodic scanning to continuous exposure monitoring, prioritising internet-facing and identity related systems.
- All exploited vulnerabilities referenced in 2025 were High or Critical, often weaponised within days.

OT and IT segmentation for manufacturing

- Ensure clear separation and monitoring between operational technology and corporate IT environments.
- Manufacturing was persistently targeted, with attackers exploiting weak segmentation to cause operational shutdowns.

Incident response planning

- Maintain up-to-date incident response plans that account for identity compromise, data theft, and service disruption.
- Many 2025 incidents escalated due to slow or fragmented response rather than technical failure alone.

Backup and recovery testing

- Regularly test backups under realistic conditions, including scenarios where encryption isn't deployed.
- Extortion without encryption rendered traditional backup strategies insufficient in several high profile cases.

Data exfiltration detection

- Deploy monitoring focused on outbound data flows, cloud storage abuse, and anomalous API activity.
- Data theft increasingly preceded or replaced encryption as the primary leverage mechanism.

Table-top exercises and rehearsals

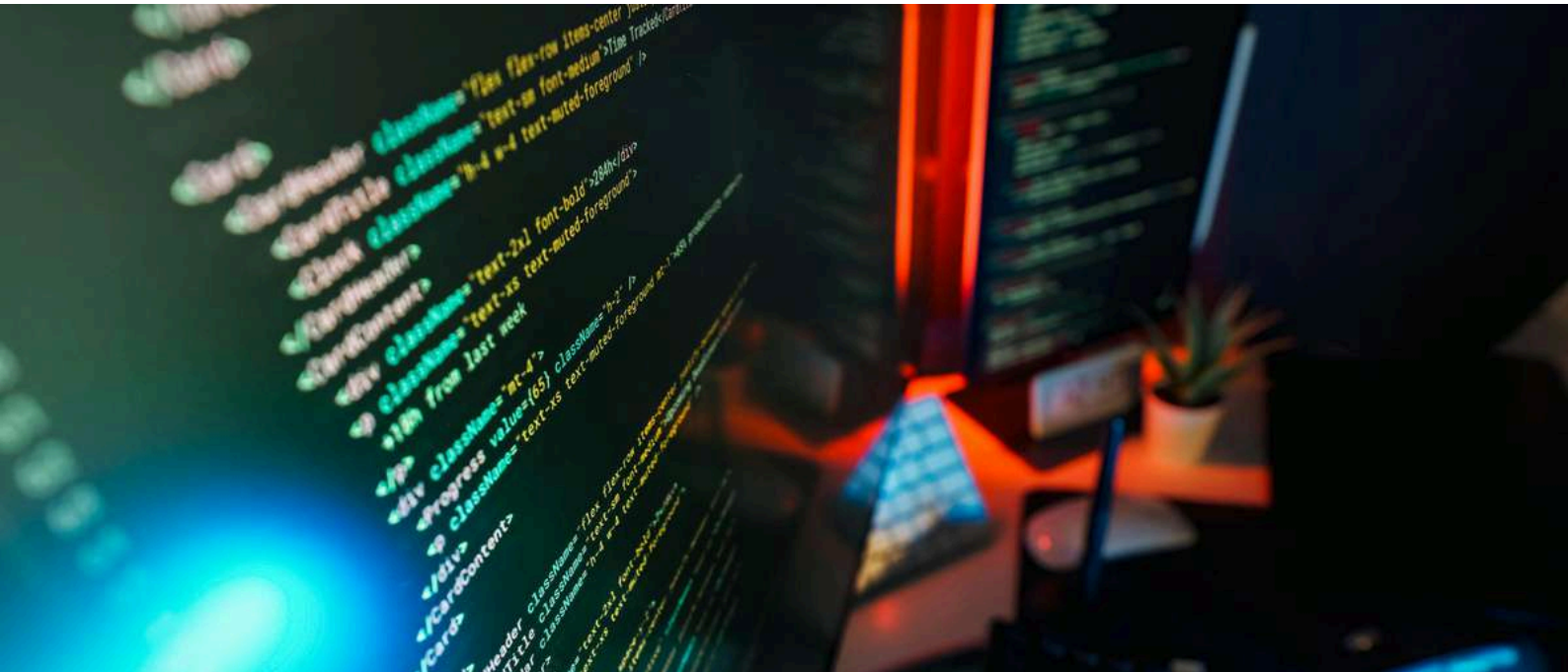
- Run cross-functional exercises involving IT, security, legal, communications, and operations.
- The most damaging 2025 incidents exposed gaps in decision making under pressure rather than purely technical weaknesses.

Supplier security assurance

- Apply minimum security standards, contractual reporting requirements, and audit rights to critical suppliers and MSPs.
- Regulatory expectations now increasingly extend accountability to the supply chain.

SOC visibility across identity and cloud

- Ensure SOC coverage includes identity telemetry, SaaS logs, and cloud control planes.
- Many 2025 attacks were malware-free and invisible to traditional endpoint-focused monitoring.



Conclusion:
Preparing for 2026

The contrast between 2024 and 2025 isn't defined by noise or volume, but by intent and execution. In 2024, many attacks were fast, visible, and malware led.

Ransomware campaigns prioritised rapid encryption, new variants appeared frequently, and compromise was often obvious within hours or days.

In 2025, attackers slowed down. They focused on stealth, persistence, and leverage. Access was gained through identity systems rather than exploits. Legitimate platforms such as SaaS tools, cloud control planes, update mechanisms, and trusted domains were used as camouflage. Dwell time increased, detection signals weakened, and the line between normal user behaviour and malicious activity became harder to distinguish.

The defining shift of the year can be summarised simply: 2025 attacks weren't louder. They were stealthier.

Cyber risk is no longer confined to data confidentiality or IT security. It's operational and geopolitical. Attacks increasingly aimed to stop organisations from functioning, disrupt public services, or apply pressure aligned to wider political or economic objectives.

Manufacturing shutdowns, aviation disruption, public sector outages, and supplier driven cascades showed that availability and trust are now primary targets.

Identity systems and supply chains must be treated as permanent attack surfaces. They are no longer secondary risks or edge cases. They are where attackers consistently succeed, particularly when combined with legitimate tooling, cloud services, and trusted relationships that sit outside traditional perimeter controls.

This reality changes the balance of defensive priorities. Prevention remains important, but it's no longer sufficient on its own. Resilience, visibility, and response capability matter more than ever. Organisations need to assume that access may be obtained, that activity may initially appear legitimate, and that business impact may unfold over days or weeks, rather than minutes.

High profile incidents during 2025, including major retail and manufacturing disruptions, reinforced this lesson. In several cases, the most damaging outcomes weren't caused by sophisticated malware, but by delays in detection, uncertainty in decision making, and a lack of rehearsed response when systems and operations were under pressure.

For 2026, the case for robust incident response planning is clear. Table-top exercises, cross functional rehearsals, and clear decision frameworks are no longer optional. They are essential for reducing impact when prevention is bypassed and for maintaining control during fast moving, high stakes incidents.

Key Takeaways:

What Did We Learn in 2025?

- Ransomware remained the most persistent threat, but extortion and disruption outweighed encryption.
- Identity abuse was the most reliable initial access method across all sectors.
- Supply-chain and SaaS compromises created the largest blast radius and fastest escalation.
- All exploited vulnerabilities referenced were High or Critical severity.
- Manufacturing, healthcare, retail and public sector organisations were consistently targeted.
- Operational disruption became a primary attacker objective, not a side effect.
- DDoS activity increasingly aligned with geopolitical events and narratives.
- Malware-free and living-off-the-land techniques reduced traditional detection effectiveness.

DigitalXRAID: Securing the Future

As cyber threats grow in complexity, DigitalXRAID remains at the forefront of cyber security innovation, offering 24/7 threat monitoring, advanced penetration testing, and industry-leading SOC services. Our expert security analysts, AI-powered threat detection, and intelligence-driven approach ensure that businesses can stay ahead of evolving cyber threats in 2026 and beyond.

Our mission remains clear:

- Protecting organisations from cybercriminals
- Ensuring business continuity despite evolving threats
- Delivering intelligence-led security solutions tailored to every industry

As we step into 2026, businesses must be prepared, proactive, and resilient. Cybersecurity is no longer just an IT function—it is a business-critical priority.

Stay Secure. Stay Resilient. Stay Ahead.

DigitalXRAID
a XYPHER company

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

---

info@digitalxraid.com **digitalxraid.com**