CASTELLUM LABS

ANNUAL THREAT REPORT

EXECUTIVE SUMMARY

2025

Threat Evolving, Defense Advancing

Table of Contents

Foreword

In 2025, the digital battlefield shifted toward the "Enterprising Adversary," a highly professionalized criminal ecosystem operating with the strategic maturity of Fortune 500 companies. As organizations transitioned to AI-native and cloud-centric operations, attackers industrialized their efforts through robust supply chains and "as-a-service" models. This evolution has created a resilience paradox: despite sophisticated defenses, "breakout times" have shrunk to under 50 minutes. The traditional network perimeter has effectively collapsed, with threat actors no longer "breaking in" but "logging in" via stolen identities and session tokens.

To counter this industrialized threat, organizations must move beyond reactive measures and treat security as a core business competency. This requires a strategic shift toward continuous exposure management, phishing-resistant authentication, and the use of Agentic AI to respond at machine speed. By replacing trust-based legacy systems with identity-centric resilience, leaders can navigate this challenging landscape and build a more secure foundation for 2026.

Purpose & Context

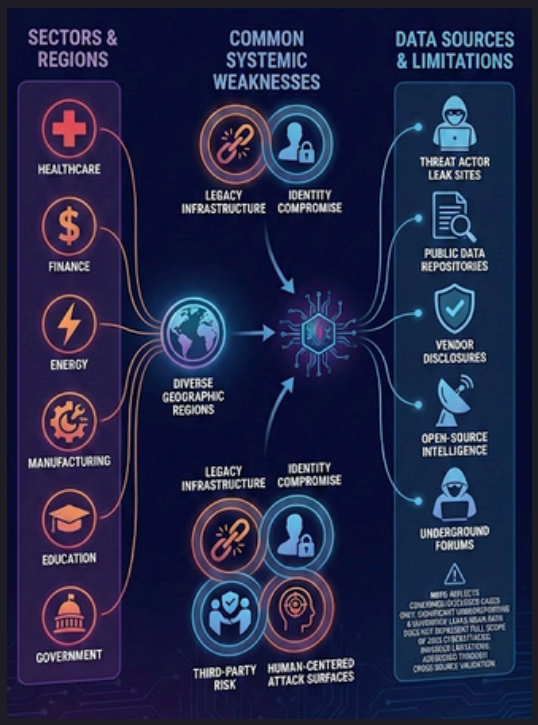
This executive summary report distills the full **Annual Threat Report 2025** by Castellum Labs into a concise, decision-focused narrative for executives, board members, and senior security leaders. It highlights the most critical trends, quantified impacts, and strategic implications observed globally in 2025.

The findings are based on Castellum Labs' comprehensive intelligence collection, which includes data from threat actor-operated leak sites, dark-web monitoring of underground forums, and detailed incident analysis. The report aims to deliver actionable insights by examining the tools, behaviors, and infrastructures powering today's threat actors, going beyond simple volume statistics to help organizations improve resilience in an increasingly complex threat environment.

2025 Global Cyber Threat Landscape

Key Metrics at a Glance

The threat landscape in 2025 was defined by unprecedented speed and the dominance of identity-based exploits.



- **Global Malware Activity:** Increased by approximately 20 - 30% year-over-year, driven primarily by infostealers and loaders.
- **Ransomware Impact:** Accounted for an estimated 35 - 40% of high-impact cyber incidents worldwide.
- **Vulnerability Exploitation:** Over 60% of investigated intrusions involved the exploitation of known or recently disclosed vulnerabilities.
- **Identity-Based Compromise:** Credential theft, session hijacking, and MFA bypass techniques were present in approximately 70% of analyzed incidents.
- **Attack Volume:** There was a >50% increase in global attack volume compared to previous periods.
- **Tactical Shift:** Over 75% of intrusions shifted toward identity-centric methods rather than traditional perimeter breaches.

Key Focus Areas

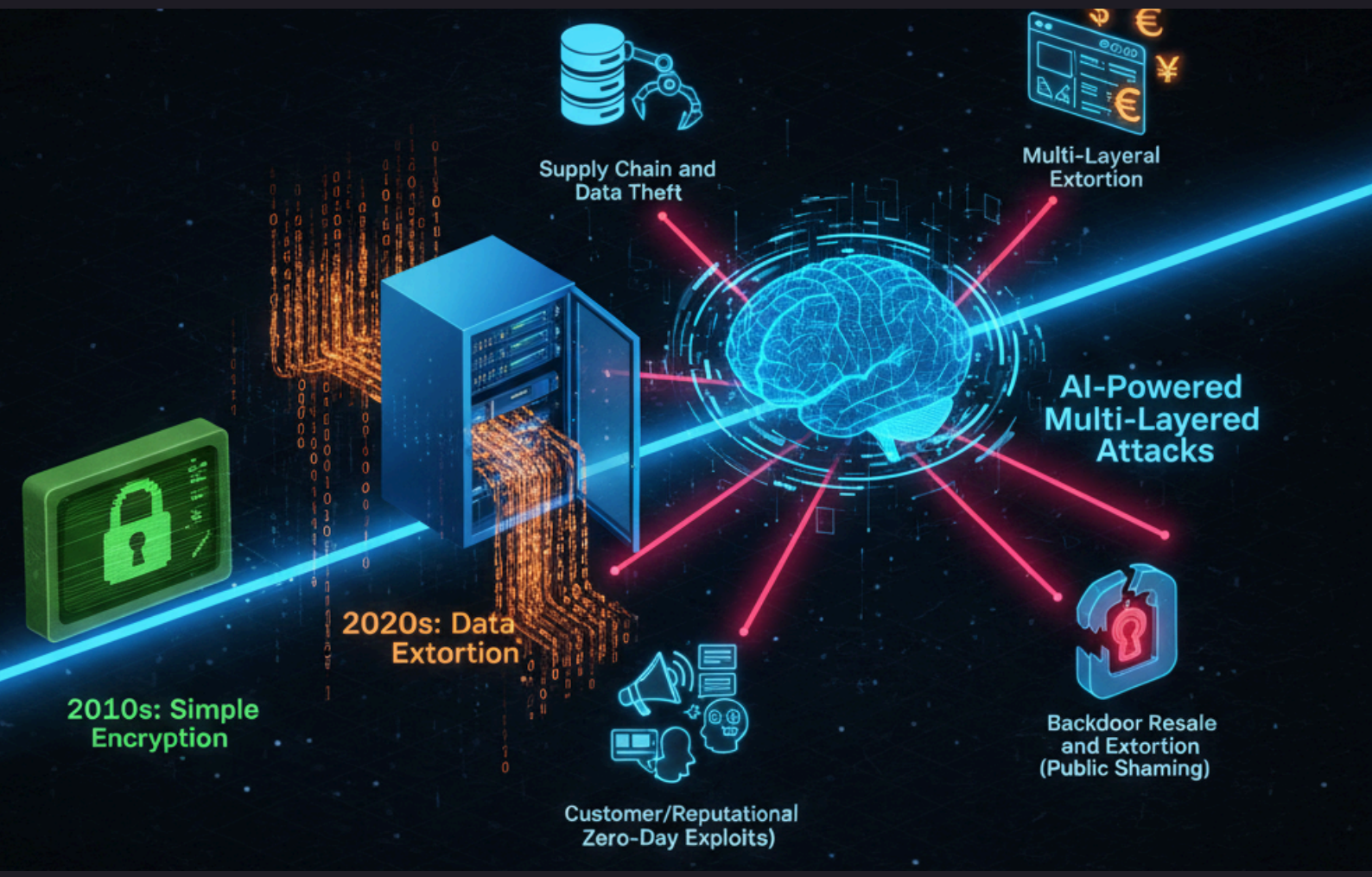
- **Industrialization of Cybercrime:** The evolution of Ransomware-as-a-Service (RaaS) into more fragmented and aggressive affiliate models.
- **Identity-Centric Shifts:** The pivot from perimeter breaches to the exploitation of harvested credentials to bypass traditional defenses.
- **Sectoral Targeting:** Analysis of disruptive attacks against high-value sectors such as manufacturing, healthcare, and critical infrastructure.
- **Tactical Evolution:** The weaponization of new vulnerabilities and the rise of "Living-off-the-Land" (LotL) techniques.

***Key Takeaway* - Speed and identity compromise were the primary drivers of attacker success in 2025.**

Global Threat Landscape Snapshot

The global cyber threat landscape in 2025 was defined by unprecedented speed, scale, and resilience. Threat actors evolved into highly professionalized, enterprise-like operations, compressing attack lifecycles and exploiting automation, stolen identities, and pre-built criminal supply chains. Despite historic law-enforcement takedowns of darknet markets, malware infrastructure, and crypto-laundering platforms, the ecosystem demonstrated a hydra-like ability to regenerate, rapidly decentralizing, rebranding, and resuming operations with minimal disruption

A critical shift in 2025 was the convergence of attack vectors and the dominance of identity-based compromise. Ransomware, malware, phishing, and social engineering now operate as integrated attack chains, with stolen credentials, session cookies, and OAuth tokens enabling attackers to bypass hardened perimeters and traditional MFA. Ransomware accounted for roughly 35 - 40% of high-impact incidents, malware activity rose 20 - 30%, and over 60% of intrusions involved exploited vulnerabilities - particularly at the network edge and in cloud environments. Together, these trends confirm that cyber risk is now continuous, identity-centric, and operational in nature, rather than perimeter-bound or episodic



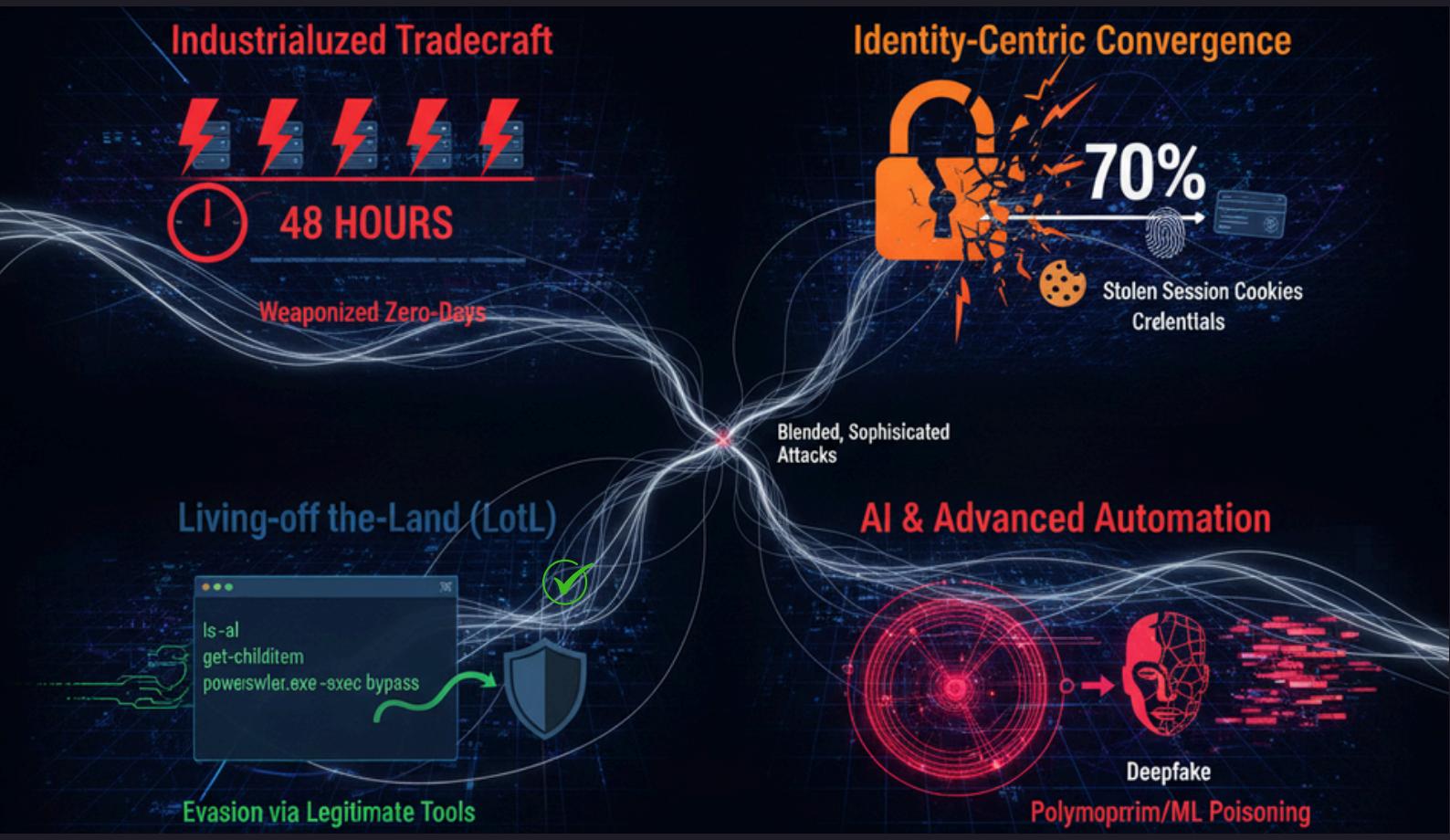
***Key Takeaway** - Cybercrime in 2025 functioned as an industrialized, highly resilient ecosystem characterized by rapid adaptation and a fundamental shift in adversary tradecraft.*

Evolution of Attack Methods

Attack methods in 2025 shifted from opportunistic campaigns to industrialized, highly evolved operations. Modern adversaries prioritized stealth, automation, and the systematic bypassing of contemporary defenses, such as Endpoint Detection and Response (EDR) and Multi-Factor Authentication (MFA).

Key Tactical Shifts:

- **Industrialized Tradecraft:** Adversaries demonstrated heightened operational maturity and faster attack cycles, often weaponizing newly disclosed vulnerabilities within days.
- **Living-off-the-Land (LotL):** There was a growing trend of abusing legitimate system tools to mask malicious activity, allowing attackers to remain undetected within compromised environments.
- **Identity-Centric Convergence**: As perimeter defenses hardened, attackers pivoted toward identity-centric intrusions. Approximately 70% of analyzed incidents involved the use of stolen credentials, session hijacking, or token abuse.
- **AI and Advanced Automation:** The landscape saw the rise of AI/ML poisoning, deepfakes, and automated infrastructure that enabled more sophisticated and persistent threats.



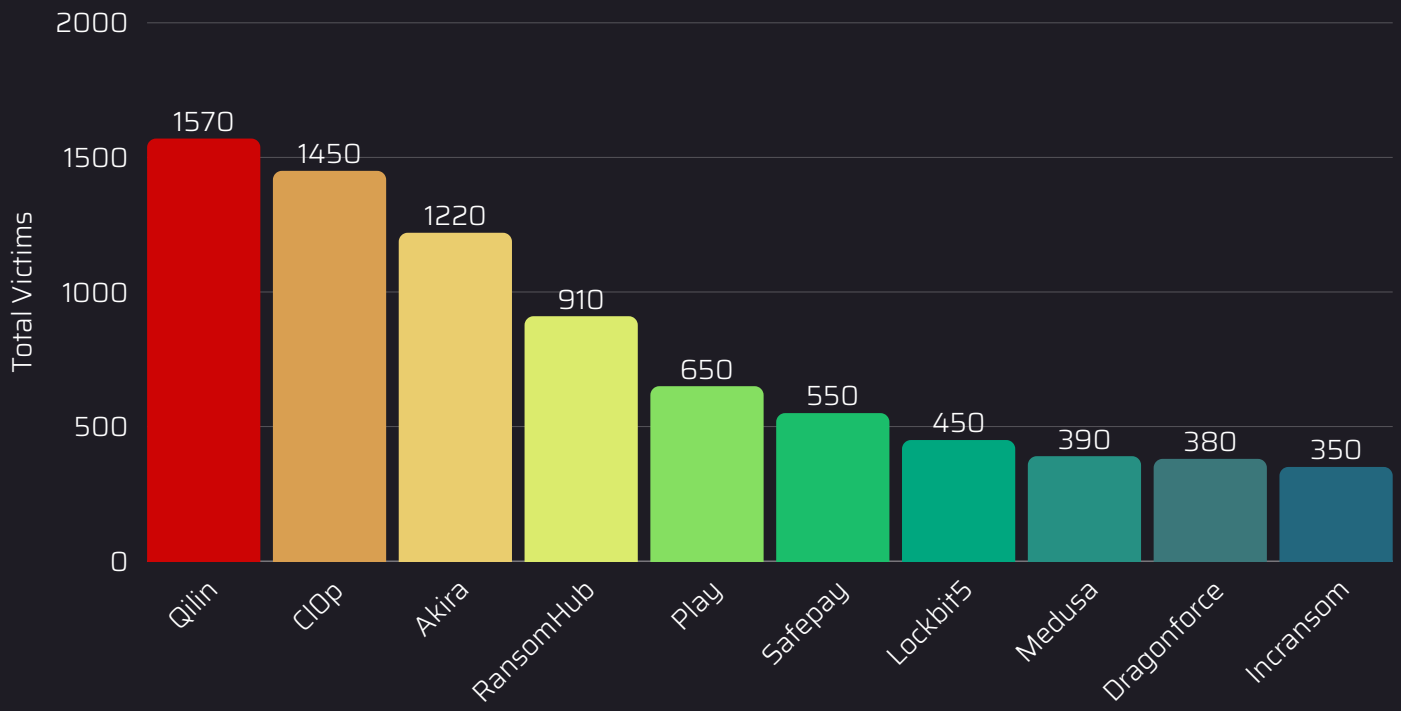
Key Takeaway - Defensive tooling alone is no longer sufficient without robust identity-centric and behavior-centric controls to counter industrialized adversary tradecraft.

Ransomware Trends 2025 : Most Active

In 2025, the ransomware landscape was characterized by high affiliate mobility and the emergence of aggressive mid-tier groups that filled the operational gaps left by disrupted legacy actors. Leading and highly active groups observed during this period included:

- **Qilin, Cl0p, and Akira:** Remained dominant players, consistently appearing on threat actor leak sites.
- **RansomHub and Play:** Maintained high-volume operations, targeting a wide range of organizations across multiple geographic regions.
- **DragonForce, Medusa, and SafePay:** Emerged as significant threats, driving disruption through aggressive data extortion and multi-layer pressure tactics.
- **Scattered Spider:** While facing significant legal pressure, including the high-profile arrest of members in the UK and US, this group remained a critical case study for high-impact social engineering and extortion, having extorted over $115 million in ransom payments.
- **LockBit:** Despite ongoing international law enforcement efforts to disrupt its infrastructure, the brand demonstrated the "hydra-like" resilience typical of 2025, with affiliates continuing to deploy variants under various guises.

Victims by the top 10 Ransomwares in 2025



Key Takeaway - The rise of agile mid-tier groups and the persistence of established brands fueled a 55 - 60% increase in active ransomware groups compared to 2024, proving that talent and operational incentives now outweigh legacy brand stability.

Ransomware: Industrialized Extortion

Ransomware remained the most disruptive threat in 2025, accounting for approximately 35 - 40% of high-impact cyber incidents worldwide. It has evolved into a sophisticated, multi-layer extortion model designed to maximize financial and operational pressure on victims.

Key Aspects of the Industrialized Model:

- **Multi-Layer Extortion:** Beyond standard encryption, threat actors employed double- and triple-extortion techniques, including data theft, the threat of public exposure on leak sites, and additional disruptive measures to compel payment.
- **Tactical Shifts:** Attackers increasingly utilized "Living-off-the-Land" (LotL) techniques, abusing legitimate system tools to mask their presence and bypass traditional security detections.
- **Weaponization Speed:** Exploitation of known or newly disclosed vulnerabilities accelerated, with attackers frequently weaponizing flaws within days of publication to gain initial access.
- **Monetization Flow:** Even with significant law-enforcement seizures of crypto-laundering hubs like Garantex, threat actors demonstrated a "hydra-like" resilience, rapidly adapting their monetization strategies.

Ransomware Market Structure

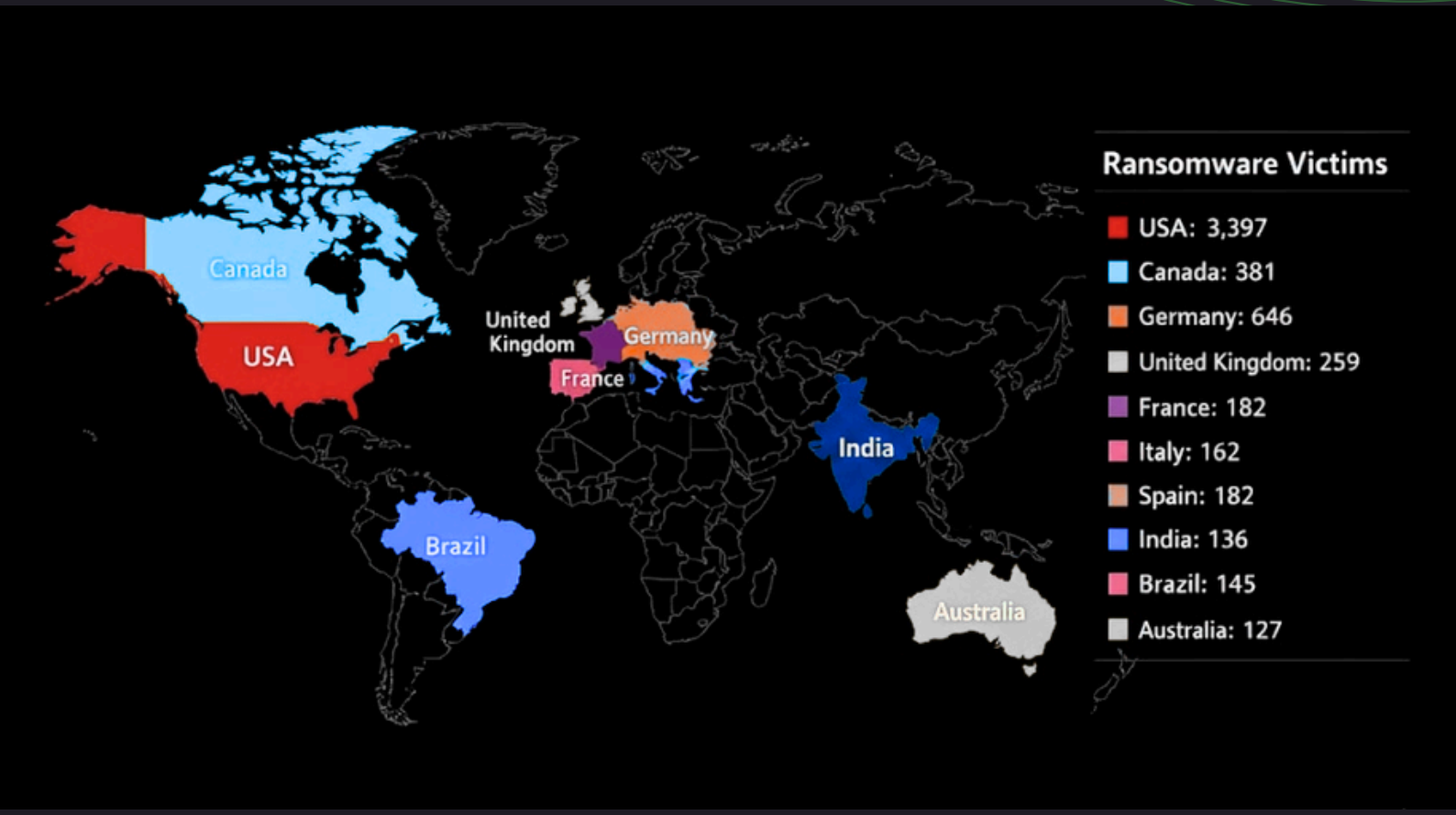
The ransomware landscape in 2025 was dominated by the mature Ransomware-as-a-Service (RaaS) model, which has become a primary driver of attack volume. This industrialized structure enables a clear division of labor between developers (operators) and the individuals who execute the attacks (affiliates).

Key Structural Characteristics

- **Affiliate Recruitment Models:** RaaS operators utilized aggressive recruitment strategies to attract skilled cybercriminals. This included offering highly competitive revenue shares, with some models observed at a 90/10 split in favor of the affiliate to incentivize high-impact intrusions.
- **High Affiliate Mobility:** The ecosystem was characterized by significant mobility, with talented affiliates frequently moving between different ransomware brands or working for multiple "employers" simultaneously. This fluid talent pool makes specific "brands" less critical than the skilled individuals behind them.
- **Market Fragmentation:** Following major law enforcement disruptions in 2025, the market saw a shift toward fragmentation. This led to the emergence of approximately 25–35 new, smaller, and often more aggressive ransomware groups.
- **Operational Resilience:** The RaaS structure allowed for "hydra-like" regeneration; when a major group was dismantled, its affiliates quickly transitioned to other existing or newly rebranded operations with minimal downtime.

Key Takeaway - In 2025, ransomware evolved beyond simple malware into a complex, industrialized business process where talent and financial incentives rather than brand loyalty drove a highly fragmented yet resilient professional ecosystem focused on high-leverage extortion.

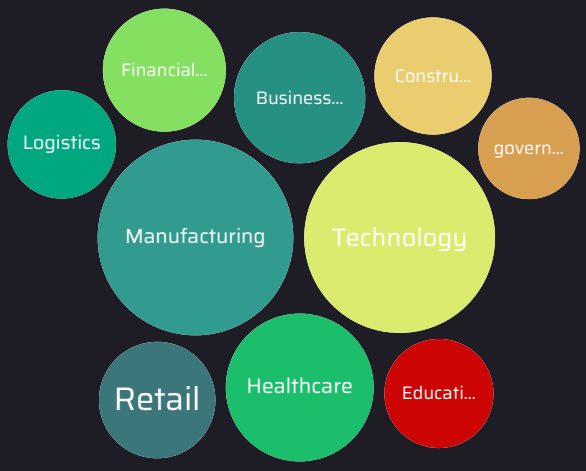
Countries most affected by Ransomware



Sectors Most Targeted by Ransomware in 2025

In 2025, ransomware targeting shifted toward sectors with low tolerance for downtime and high-value proprietary data. According to consolidated telemetry from global incident response firms and dark web leak site monitoring, the following five sectors were the most targeted.

- Widespread use of cloud services, remote access, and third-party tools increased exposure to ransomware in 2025.
- Availability of large amount of sensitive confidential data.
- Operational disruption creates urgency, forcing organizations to respond quickly to restore critical services.

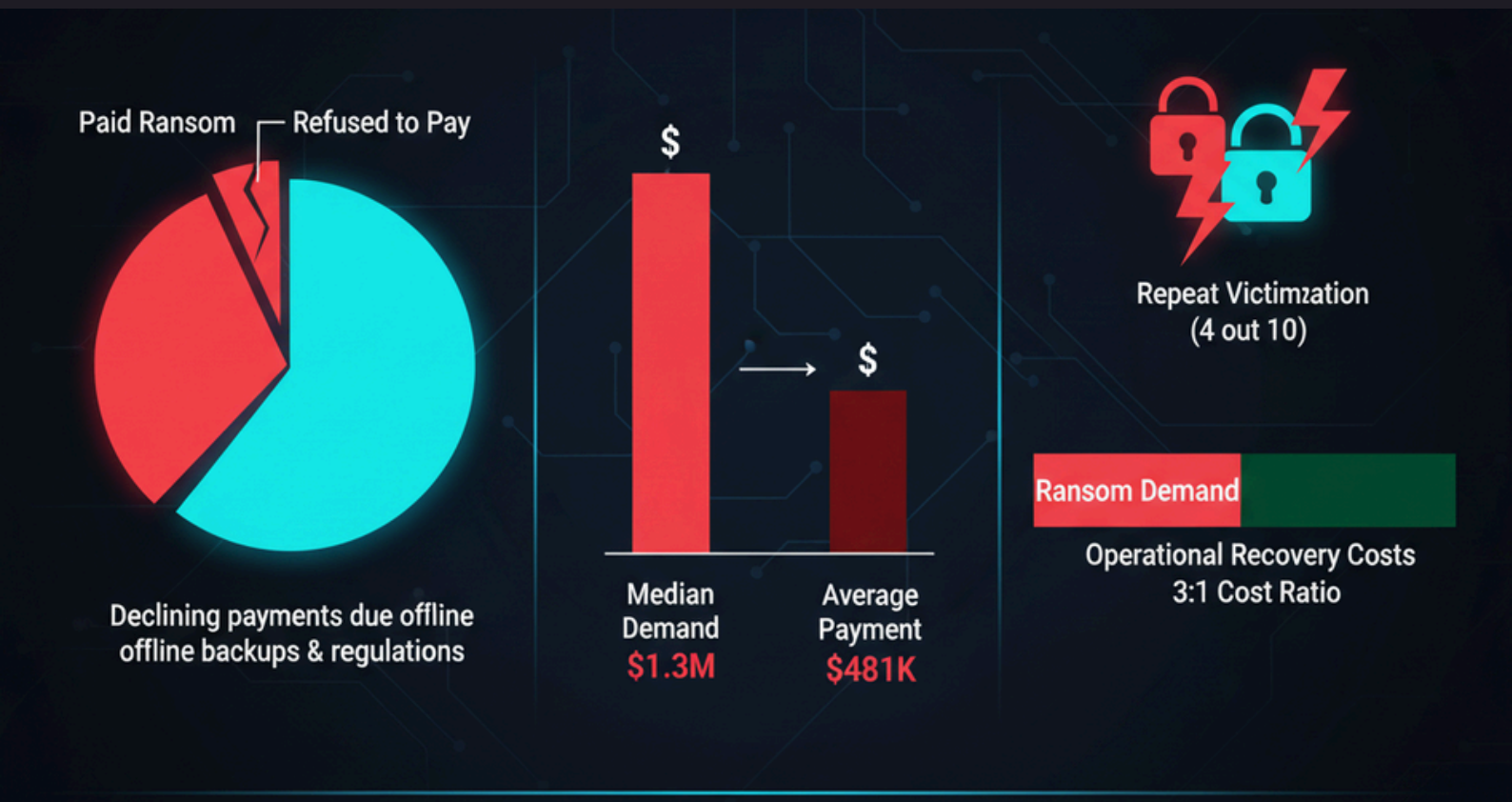


Ransomware Economics

The financial landscape of ransomware in 2025 reflected a shift toward high-volume, industrialized extortion. While the "big game hunting" of massive corporations continued, the broader market stabilized into a predictable - yet devastating - business model.

Financial Benchmarks in 2025

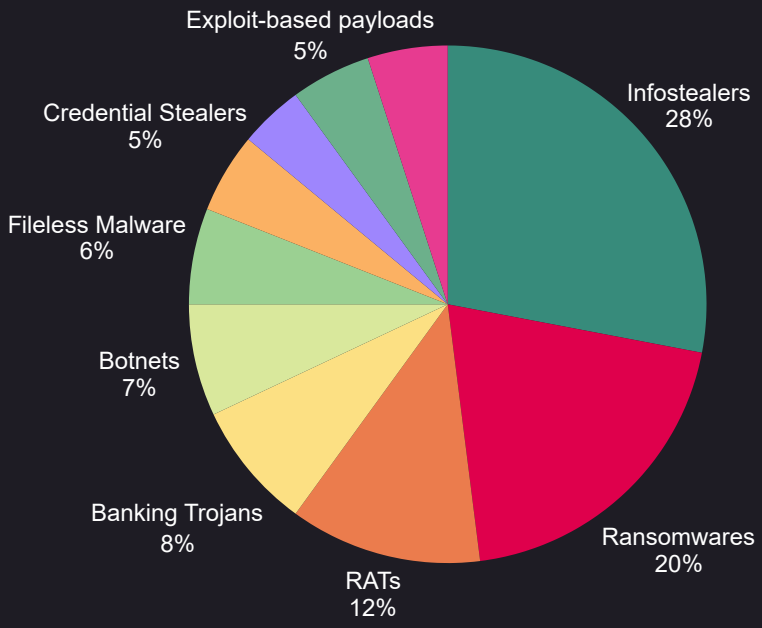
- **Declining Propensity to Pay:** Fewer than 30% of victims chose to pay the ransom, down from previous years. This shift is attributed to better offline backup strategies and increased regulatory pressure against funding criminal entities.
- **Ransom Demands:** The median initial ransom demand hovered around USD 1.3 million, though demands for critical infrastructure targets often reached eight figures.
- **Average Payment:** For those who did pay, the average settlement was approximately USD 481,000, as victims became more proficient at negotiating and partial data recovery.
- **Repeat Victimization:** A disturbing trend in 2025 saw a rise in "re-extortion," where victims were targeted by a second group (or the same group under a different brand) shortly after the first incident, often using the same initial access point.
- **Operational Recovery Costs:** Organizations reported that the cost of downtime, forensic investigations, and legal fees typically outweighed the ransom demand by a factor of 3 to 1.



Key Takeaway - Attackers have shifted to volume-based extortion to compensate for lower payment rates, making ransomware a game of persistence and operational disruption rather than just data encryption.

Malwares Trends 2025: Most Active

In 2025, malware became increasingly modular and service-driven, adapting to bypass traditional security measures. Global malware activity rose by approximately 20–30% year-over-year.



Key Malware Characteristics

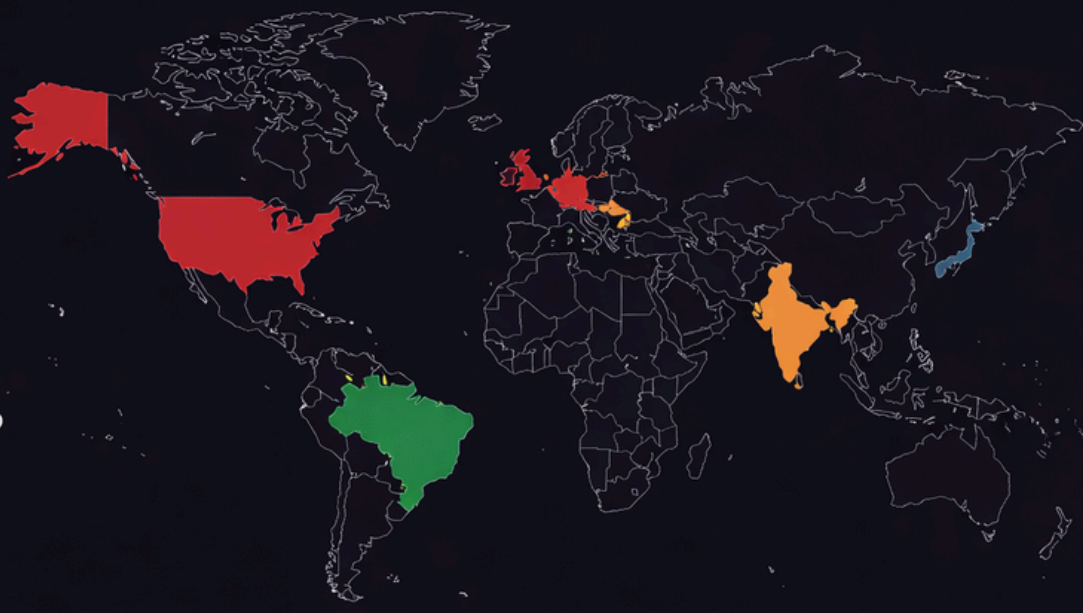
- **Modular Attack Chains:** Threat actors increasingly relied on modular chains where initial-access malware facilitated credential theft and lateral movement, ultimately enabling monetization through ransomware or data extortion.
- **Dominance of Loaders and Infostealers:** These families, such as the Lumma-type stealers, scaled rapidly, enabling tens of thousands of infections that directly fueled broader fraud and account takeover campaigns.
- **Initial Access Enablers:** Between 40 and 60 new malware families were identified in 2025, with the majority focused on credential harvesting and serving as enablers for follow-on intrusions.
- **Stealth and Evasion**: Attackers favored "Living-off-the-Land" (LotL) techniques, abusing legitimate system tools to mask their malicious activity and evade detection.
- **Emerging Highly Evolved Threats:** The landscape saw the rise of advanced methods, including AI/ML poisoning, deepfakes, and automated infrastructure, which represent the next phase of evolved cyber threats.

Key Takeaway - With the shift toward modular, service-driven malware and the use of legitimate system tools, signature-based defenses have become largely ineffective against modern, industrialized malware operations.

Countries most affected by Malwares (2025)

Malware Attack Distribution:

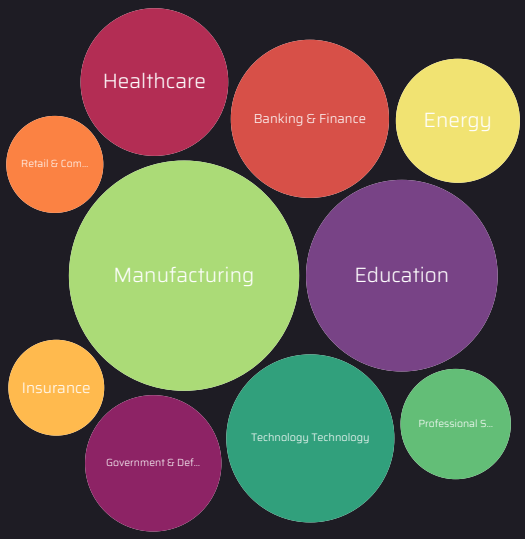
- United States: 30%
- India: 9%
- Ukraine: 12%
- Israel: 7.5%
- Japan: 6%
- United Kingdom: 5.5%
- Saudi Arabia: 4.5%
- Brazil: 4.25%
- Germany: 4%
- Poland: 3.75%



Sectors most affected by malwares

In 2025, non-ransomware malware - including Information Stealers, Remote Access Trojans (RATs), and Cryptominers - accounted for the largest volume of global cyber incidents. These attacks prioritized long-term persistence, data exfiltration, and resource hijacking over immediate disruption.

- In 2025, Manufacturing was targeted due to digitalization and OT/IT convergence, providing entry points for ransomware, espionage, and supply chain attacks.
- Healthcare sector were targeted because of their sensitive data & decentralized IT environments.
- BFSI sectors were attacked for credential theft, data exfiltration, and financial gain



Dark Web & Criminal Economy

The dark web matured into a professional, highly resilient B2B ecosystem in 2025, demonstrating a "hydra-like" capacity to regenerate despite significant law enforcement pressure. This illicit economy is now characterized by an industrialized supply chain where specialized actors provide the tools and access necessary for high-impact attacks.

Key Components of the 2025 Criminal Economy:

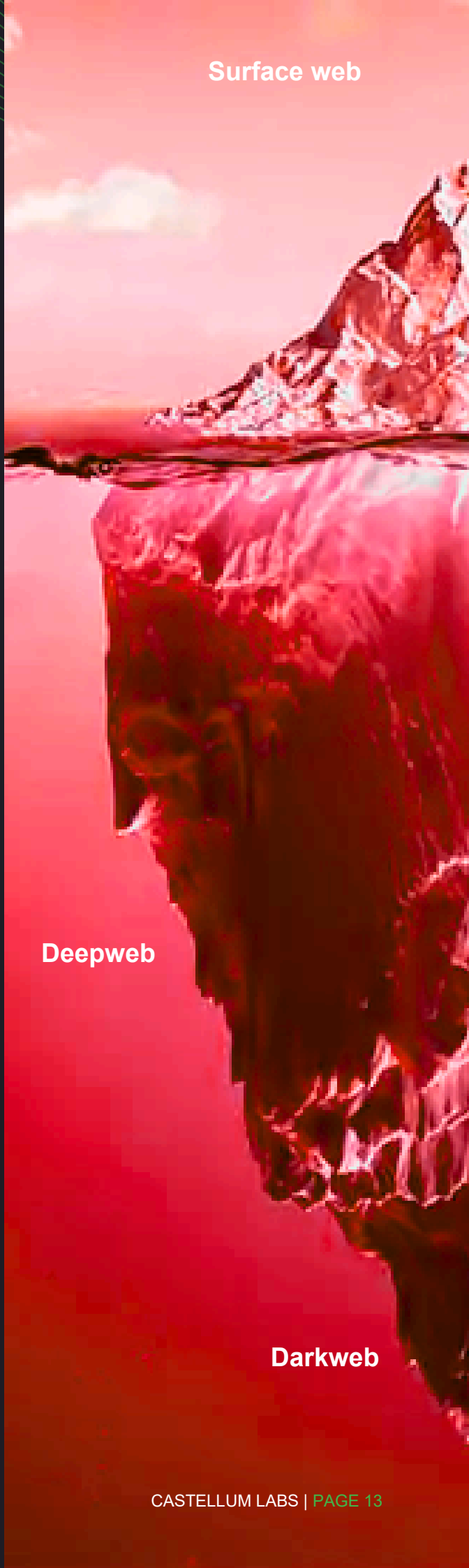
- **Initial Access Brokers (IABs):** Specialized actors who focus on breaching organizations and selling that verified access - such as VPN credentials or web shell access - to other cybercriminals, including ransomware affiliates.

- **Malware-as-a-Service (MaaS):** The ecosystem saw the proliferation of modular malware families. Developers offered sophisticated loaders and infostealers, like the Lumma-type families, which enabled tens of thousands of infections for follow-on fraud and account takeovers.

- **Ransomware-as-a-Service (RaaS):** This model evolved into more fragmented and aggressive affiliate structures, allowing threat actors to rapidly restructure and rebrand following infrastructure takedowns.

- **AI-Powered Cybercrime Tools:** The availability of AI-driven tools on underground forums facilitated more effective social engineering, deepfakes, and automated attack infrastructure.

- **Professionalized Services:** Beyond malware, the dark web provided specialized services such as crypto-laundering hubs (e.g., the seized Garantex platform) and bulletproof hosting to mask malicious operations.



Infostealers & Identity Theft

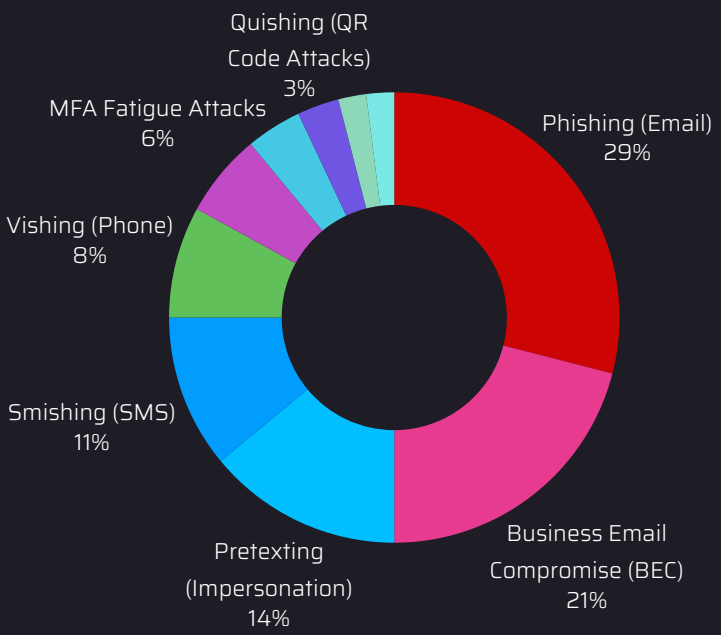
In 2025, infostealers became a primary driver for major cyberattacks by systematically harvesting critical authentication data. These tools enabled threat actors to move beyond simple credential theft to sophisticated identity-centric intrusions.

Core Data Targeted by Infostealers:

- **Browser Credentials:** Harvesting stored usernames and passwords directly from compromised systems to fuel account takeover campaigns.
- **Session Cookies:** Stealing active session data to bypass multi-factor authentication (MFA) through session hijacking.
- **OAuth Tokens:** Exploiting third-party authentication tokens to gain persistent access to cloud and SaaS environments without needing a password.
- **Crypto Wallets:** High-volume theft from digital wallets, with families like Rhadamanthys alone accessing over 100,000 crypto wallets.

Impact on Security: The rapid scale of infostealer families, such as Lumma-type stealers, enabled tens of thousands of infections that served as initial access enablers for follow-on ransomware and fraud operations. By focusing on these identity artifacts, attackers effectively rendered traditional perimeter defenses and standard MFA less effective.

Top 10 Social Engineering Attacks 2025

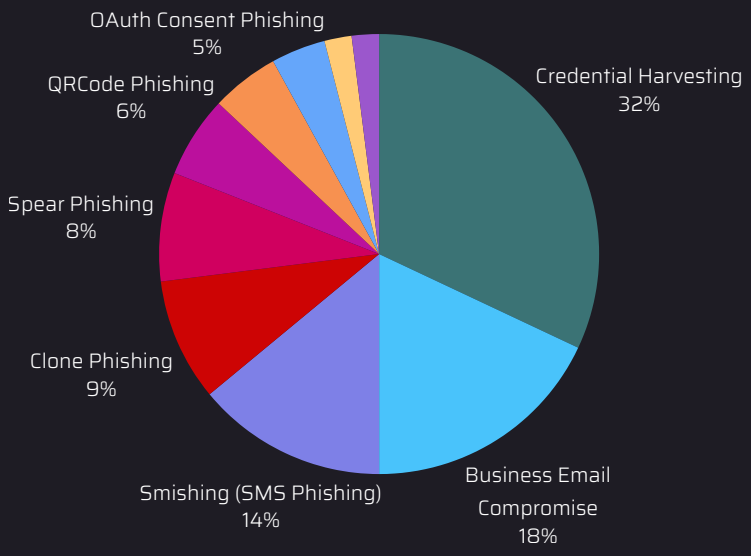


Key Takeaway - Identity is now the primary attack surface, with infostealers providing the "keys to the kingdom" through session and token abuse.

Phishing & Social Engineering Trends in 2025

Phishing and social engineering reached new levels of effectiveness in 2025, remaining a top attack vector alongside ransomware and identity-based intrusions. These campaigns became increasingly sophisticated, moving beyond simple lures to highly industrialized operations.

Top 10 Phishing Attacks (2025)



Key Drivers of Phishing Effectiveness

- **Generative AI Content:** Attackers leveraged AI to create highly convincing, error-free, and personalized content, making it nearly impossible for users to distinguish fraudulent messages from legitimate communications.
- **Localization and Personalization:** Campaigns were tailored with precise regional context and personal data harvested from previous breaches, significantly increasing success rates.
- **QR-Code Phishing (Quishing):** The use of malicious QR codes grew as a tactic to bypass traditional email security filters and move the attack to a user's mobile device.
- **Multi-Channel Lures:** Attackers utilized integrated attack chains across email, SMS (smishing), and social media to establish trust and persistence with targets.
- **Human-Centered Attack Surfaces:** Threat actors continued to exploit human behavior and systemic weaknesses, targeting individuals in high-risk sectors like healthcare and manufacturing.

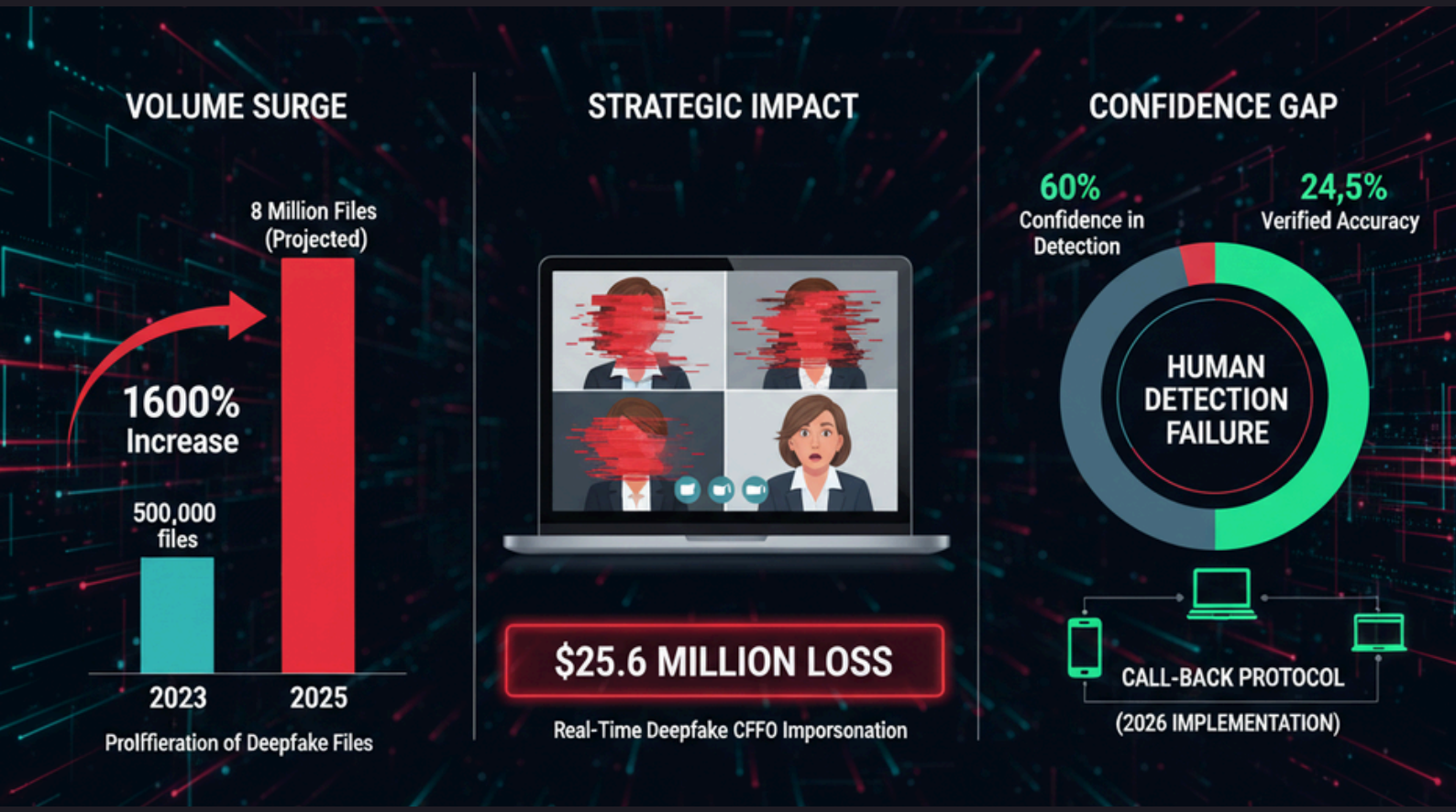
Key Takeaway - The industrialization of phishing, powered by AI and multi-channel strategies, means that human detection alone is no longer a reliable defense against modern social engineering.

Deepfakes & Vishing

The integration of artificial intelligence into social engineering significantly heightened the threat landscape in 2025, particularly through the use of deepfakes and advanced vishing (voice phishing).

Tactical Evolution of Impersonation:

- **Real-Time Voice Cloning:** Adversaries utilized AI-powered voice cloning to conduct highly sophisticated vishing attacks, enabling the impersonation of trusted figures such as corporate executives.
- **Executive Impersonation:** These tools allowed threat actors to convincingly mimic senior leadership during high-stakes communications to authorize fraudulent actions.
- **Fraudulent Wire Transfers:** Social engineering campaigns, powered by AI-generated audio and video, were used to deceive employees into initiating large-scale unauthorized financial transfers.
- **MFA Interception:** Voice cloning and AI-driven disinformation campaigns were leveraged to intercept or manipulate Multi-Factor Authentication (MFA) processes, further compromising account security.



Key Takeaway - As AI continues to evolve, voice and video are no longer reliable authentication factors, requiring organizations to adopt more robust, multi-layered identity verification methods.

Initial Access & Edge Exploitation

In 2025, the network edge became a primary battlefield as threat actors shifted their focus toward exploiting infrastructure that sits outside the traditional internal security perimeter. Attackers demonstrated high proficiency in identifying and weaponizing vulnerabilities in edge devices to gain persistent access to corporate environments.

Key Targets for Initial Access

- **Virtual Private Networks (VPNs)**: Compromising VPN gateways remained a top priority for attackers seeking to bypass perimeter security and establish a foothold within the network.
- **Managed File Transfer (MFT) Tools**: High-value MFT platforms were frequently targeted due to the concentration of sensitive data they handle, often serving as a single point of failure for massive data exfiltration.
- **Firewalls and Edge Gateways:** Vulnerabilities in security appliances were exploited to disable protections or create backdoors for lateral movement.
- **Zero-Day Weaponization:** A critical trend in 2025 was the speed of exploitation. Over 60% of investigated intrusions involved the exploitation of vulnerabilities, with many being weaponized within days - or even hours - of disclosure.

Key Takeaway - Perimeter exposure remains a critical systemic weakness; the speed at which attackers now weaponize edge vulnerabilities outpace the traditional patching cycles of most organizations.

Cloud & SaaS Attacks

As organizations continued their migration to cloud-native architectures in 2025, threat actors pivoted their focus to exploit the unique vulnerabilities of these environments. The report highlights that cloud security is no longer just about infrastructure but is fundamentally tied to identity and configuration.

Primary Cloud Attack Vectors:

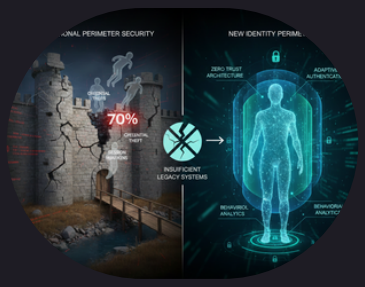
- **Misconfigurations**: Publicly exposed storage buckets and insecure API endpoints remained the most common entry points, often discovered by attackers using automated scanning tools.
- **OAuth Abuse:** Attackers increasingly shifted toward stealing or tricking users into granting malicious OAuth tokens. This allowed persistent access to SaaS applications (like Email and CRM) without the need to bypass traditional MFA or know the user's password.
- **Credential Theft & Token Hijacking:** By stealing session tokens from local machines via infostealers, attackers successfully bypassed hardware-based security keys and moved laterally into cloud management consoles.
- **Management Plane Compromise:** High-impact incidents involved the compromise of administrative accounts with "God-mode" privileges, enabling attackers to wipe entire cloud environments or hold cloud-hosted backups for ransom.

Key Takeaway - Cloud security is now an identity battle; a single compromised session token or OAuth misconfiguration can lead to a total lockout of organizational data and services.

Strategic Risks for Organizations

In 2025, systemic vulnerabilities became the primary leverage points for industrialized threat actors. The report identifies several critical weaknesses that consistently facilitated high-impact breaches and large-scale data exfiltration.

Key Systemic Weaknesses



- **Identity Security Gaps:** Identity-based attacks dominated intrusion paths, with credential theft, session hijacking, and MFA bypass present in approximately 70% of analyzed incidents. The shift toward identity-centric compromise has rendered traditional perimeter-focused security models insufficient.

- **Patch Latency and Asset Visibility:** Persistent gaps in patch management and exposure reduction - especially for internet-facing systems and edge infrastructure allowed attackers to weaponize newly disclosed flaws within days. Over 60% of investigated intrusions involved the exploitation of such vulnerabilities.

- **Legacy Infrastructure:** Threat actors repeatedly exploited legacy systems that lack modern security controls, providing an easier point of entry and persistent foothold within organizational networks.

- **Over-reliance on Perimeter Defenses:** As adversaries pivoted to identity-centric attacks and "Living-off-the-Land" (LotL) techniques, organizations relying solely on perimeter hardened defenses found themselves vulnerable to attackers using valid, harvested credentials to bypass detection.

- **Third-Party and Supply Chain Risk:** Compromises in the vendor ecosystem and third-party tools (such as Managed File Transfer platforms) were used to gain broad access to multiple downstream victims simultaneously.

- **Inadequate Backup Isolation:** Attackers prioritized the compromise of cloud management consoles and administrative accounts to delete or encrypt backups, significantly increasing their extortion leverage.

Key Takeaway - Cyber resilience must be systemic and behavior-centric, rather than tool-driven. Organizations must move beyond the perimeter and focus on securing the identity layer and reducing the technical debt of legacy systems.

Conclusion & Strategic Recommendations

The 2025 threat landscape demonstrates that cybercrime has fully matured into an industrialized, identity-driven ecosystem where speed, scale, and adaptability determine attacker success. With over 70% of incidents involving credential theft, session hijacking, or token abuse, and breakout times shrinking to under an hour, the traditional network perimeter is no longer a meaningful line of defense. Ransomware has evolved beyond encryption into multi-layer extortion, while law-enforcement takedowns have proven disruptive but insufficient to dismantle a hydra-like criminal supply chain. The convergence of ransomware, malware, phishing, AI-driven social engineering, and cloud exploitation confirms that cybersecurity can no longer be reactive or tool-centric. To remain resilient, organizations must adopt an identity-first, exposure-aware, and automation-driven security strategy that assumes breach inevitability and prioritizes operational continuity over prevention alone

Strategic Priorities for 2026:

- **Adopt an Identity-First Security Model:** Since identity is now the primary attack surface, organizations must prioritize robust identity governance. This includes moving beyond basic MFA to phishing-resistant authentication and implementing continuous session monitoring to combat token theft.
- **Implement Continuous Threat Exposure Management (CTEM):** Shift away from static, periodic patching cycles. Organizations should adopt automated, real-time visibility of their attack surface, prioritizing the remediation of edge infrastructure and internet-facing assets.
- **Operationalize AI-Native Defenses:** As attackers use AI to accelerate their breakout times (now averaging under 50 minutes), defenders must use AI-driven security operations (SOC) to automate detection, correlation, and response at machine speed.
- **Eliminate Technical Debt:** Systemic risks are often rooted in legacy systems that lack modern telemetry. Replacing end-of-life (EOL) software and hardware is a fundamental security requirement, not just an IT upgrade.
- **Strengthen Supply Chain Governance:** Vet third-party vendors with the same rigor as internal systems. Focus on the security of Managed File Transfer (MFT) tools and remote access points used by partners.
- **Build a Culture of Resilience:** Assume breaches are inevitable. Focus on "Resilience by Design" by ensuring offline, immutable backups are secure and that incident response plans are field-tested against modern multi-layer extortion tactics.

Final Takeaway

The findings of the Annual Threat Report 2025 make one conclusion unmistakably clear: cybercrime has evolved into a fully industrialized, identity-driven business ecosystem, and traditional security models are no longer sufficient to counter it. The modern adversary operates with the discipline, scalability, and strategic intent of a legitimate enterprise - leveraging Ransomware-as-a-Service, Initial Access Brokers, infostealers, and AI-assisted automation to execute attacks at unprecedented speed. With breakout times now averaging under 50 minutes, and more than 70% of analyzed incidents involving credential theft, session hijacking, or MFA bypass, the legacy concept of a hardened network perimeter has effectively collapsed.

Throughout 2025, attackers demonstrated that valid identities - not malware alone - are the most powerful intrusion tools. Stolen credentials, session cookies, and OAuth tokens enabled adversaries to bypass perimeter defenses, EDR tools, and traditional MFA with alarming consistency. At the same time, ransomware matured from simple encryption into a multi-layer extortion model, combining data theft, public exposure, operational disruption, and repeat victimization. Even large-scale law enforcement actions and infrastructure takedowns, while disruptive, proved insufficient to dismantle the ecosystem, which rapidly regenerated through decentralization, rebranding, and affiliate mobility.

The convergence of ransomware, malware, phishing, deepfake-enabled social engineering, and cloud exploitation confirms that cybersecurity risk is no longer episodic or technical in nature - it is continuous, operational, and directly tied to business resilience. Edge infrastructure, cloud management planes, third-party tools, and legacy systems have become systemic points of failure, while sectors with low tolerance for downtime - manufacturing, healthcare, critical infrastructure, and public services - have borne the greatest impact.

To counter an adversary that operates like a business, organizations must respond in kind. Cybersecurity must be elevated from a technical silo to a core business strategy, driven by leadership accountability and sustained investment. This requires an identity-first security model, continuous threat exposure management, AI-enabled detection and response at machine speed, and a deliberate reduction of technical debt. Most critically, organizations must assume breach inevitability and design for resilience - ensuring that even when intrusions occur, they do not escalate into material business disruption. In the era of the enterprising adversary, resilience - not prevention alone - is the defining measure of security maturity.

CISO Strategic Cheat Sheet: 2026 Resilience Roadmap

The "Industrialized Adversary" now operates with business-like efficiency. This cheat sheet translates technical findings into board-level strategic priorities.

1. Executive Summary: The 2025 Reality Check

- **The "Hydra" Effect:** Takedowns only cause temporary friction. Attackers now rebrand and restructure in days, not months.
- **Identity is the Perimeter:** 70% of breaches involved identity compromise (session hijacking, OAuth abuse, or credential theft).
- **Speed is the Defining Risk:** Weaponization of edge vulnerabilities now occurs within 24–48 hours of disclosure.
- **Industrialized Extortion:** Ransomware has moved beyond encryption to a multi-layered business model (data theft + public shaming + DDoS).

2. Board-Level "Elevator Pitch"

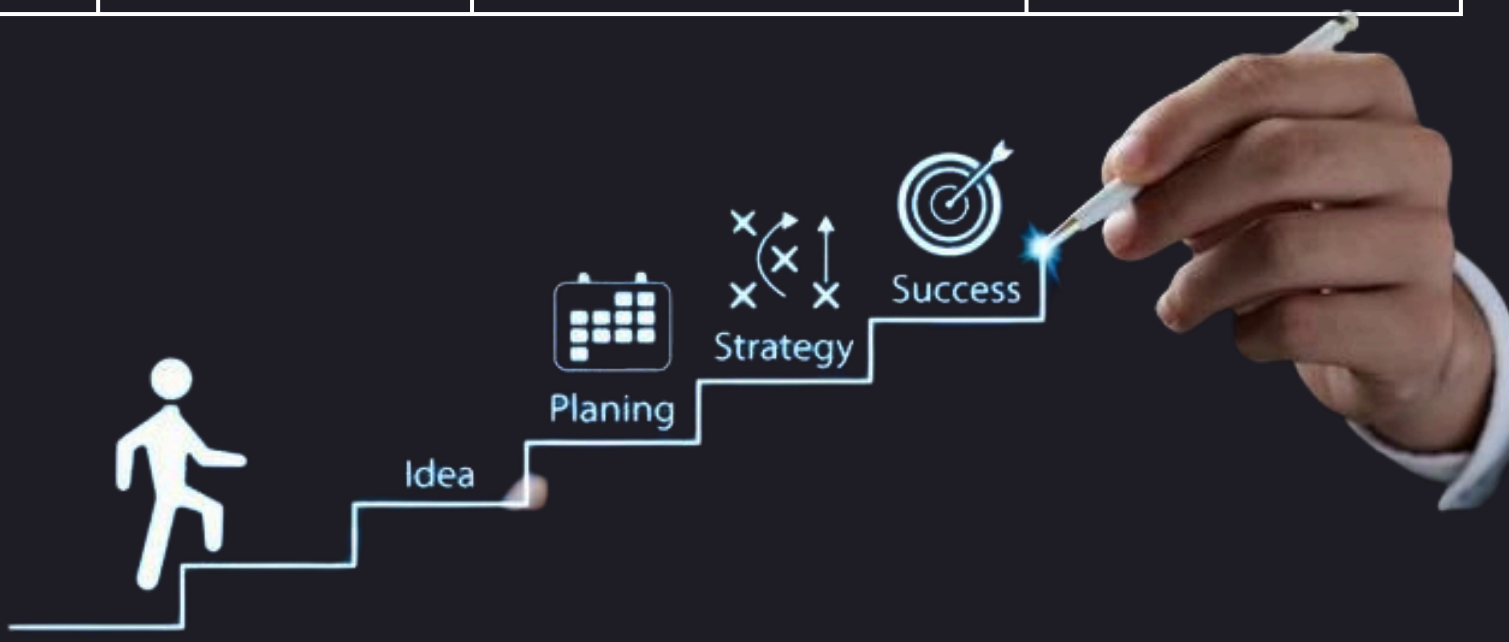
"In 2025, we saw cybercrime become a professionalized industry. We can no longer prevent every entry, so our strategy for 2026 shifts from Static Defense to Operational Resilience. We are investing in identity security to neutralize stolen credentials and AI-driven automation to respond at the speed of the attacker. Our goal is to ensure that even if a breach occurs, it never becomes a material business disruption."

3. Immediate Action Items (The "Monday Morning" List)

- **Audit Non-Human Identities:** Identify and rotate service accounts/API keys—the fastest-growing attack vector.
- **Isolate Backup Planes:** Ensure backups are on a completely different identity provider/network from production.
- **Deepfake Simulation:** Run a tabletop exercise involving a simulated "Voice Clone" of the CEO requesting a wire transfer.
- **Zero-Day Playbook:** Establish a "Fast-Track" patching process specifically for edge devices (VPNs, Firewalls, MFTs).

4. Top 5 Strategic Priorities for 2026

S.no	Priority	Strategy	Success Metric
1.	Identity Resilience	Move beyond legacy MFA to Phishing-Resistant MFA (FIDO2) and Continuous Session Validation.	> 85% of identities under phishing-resistant MFA.
2.	Exposure Management	Implement Continuous Threat Exposure Management (CTEM) to replace quarterly scanning.	Mean Time to Remediate (MTTR) < 48 Hours (Industry average is currently 5–7 days) for critical edge assets.
3.	AI-Native SOC	Deploy Agentic AI to automate triage and containment; shift human talent to high-level strategy.	Detection Breakout Time Target: < 30 Minutes (Current attacker average is ~50 mins).
4.	Cloud Sovereignty	Secure the Management Plane; treat cloud misconfigurations as a "P0" prevention priority.	Zero high-risk unauthenticated cloud APIs. (100% Remediation of "P0" risks within 4 hours.)
5.	Supply Chain Trust	**Operationalize Continuous Assurance for vendors; move from surveys to real-time control validation.**	**> 60% of critical vendors providing continuous telemetry. (Currently only ~15-20% for most enterprises)**



About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!

Cyber Security Portfolio

Secure Cloud WL	24x7 Monitoring	Vuln Mgmt	Threat Intel	Data & Privacy
Design Security for Cloud	MDR, 24x7 Monitoring	Application Security	Threat Intel Solutions	Data Security Design
Cloud Security Posture	SOC as a Service	Network VAPT	Darkweb Hunting	Data Sec Posture Assmnt
DevOps Infra Security	SIEM/SOC Design & Impl	Cloud VAPT	Deep Intel Reports	Data Sec Posture Mgmt
Container Security	SOC Team on Hire	Controls & Config Audit	Threat Intel Integrations	Encryption Design & Sol
Kubernetes Security	Managed Incidents	Program Design for VAPT	Intelligence Automations	Data Exfiltration Assmnt
Integrated S/W Security	IR Process Designs	Managed Vuin Programs	Threat Intel Curation	Privacy Designing
Workload Hardening	IR Workshops	VAPT Automations	Vectored Searches	Privacy Gap Assessment
Security Automation	SOC Assessments	Surface Assessments	Data Hunting	Privacy Adoption Service
Cloud Native Monitoring	Threat Hunting Services	Threat Intel for VAPT	Threat Intel Architecture	Privacy Automations
Cloud Governance	Forensic Services	DevSecOps	Adversary Tracking	Privacy Compliances
We create secure cloud environments, automate Cloud SecOps & manage it.	**When it comes to SOC Monitoring & Response, we cover all aspects of it**	**Program designed VAPT Engagement to enhance protection & reduce attack surface**	**We take threat intel maintenance, keep, usage & application to next level.**	**Data and privacy are two considerations, we design, implement it & run compliances**

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 8639953505