The Five Most Prevalent Cyber Attacks as of July 2025

Executive Summary

As of July 2025, the cybersecurity landscape is characterized by a dynamic and increasingly sophisticated array of threats. Analysis of leading threat intelligence reports reveals five dominant cyber attack types that pose the most significant risk to organizations globally. These include AI-enhanced phishing and social engineering, identity-based attacks, the rapid exploitation of vulnerabilities, sophisticated ransomware and extortion, and pervasive supply chain attacks. A critical commonality across these threats is the pervasive influence of Artificial Intelligence (AI), which acts as a force multiplier for adversaries, enabling more personalized, scalable, and stealthy campaigns. To effectively counter these evolving challenges, organizations must transition towards integrated, AI-driven, and resilience-focused security strategies that encompass advanced threat detection, robust identity management, and comprehensive third-party risk assessment.

Table 1: Top 5 Common Cyber Attacks (July 2025) - Overview

Attack Type	Primary Characteristics	Key Data/Statistics	Primary Impact
1. AI-Enhanced Phishing, Social Engineering, and Automated Attacks	Leverages AI for highly convincing deepfakes, vishing, and automated reconnaissance. Lowers entry barrier for attackers.	Vishing attacks are up 442% (H2 2024).[1] AI-generated emails 54% click-through vs. 12% for human.[1] Active scanning up 16.7% globally.[3]	Erosion of trust, widespread deception, scaled initial access, prolonged detection times.
2. Identity-Based Attacks and Stolen Credentials	Exploits valid accounts, fueled by infostealer malware and access brokers. Often malware-free ("hands-on-keyboard").	30% of total intrusions used valid accounts.[4] Infostealers via phishing up 84% YoY.[4] Stolen credentials 2nd most common initial vector (16%).[5] 79% of detections malware-free.[2]	Stealthy, persistent access; lateral movement; prolonged dwell times; direct access to sensitive data and cloud environments.
3. Exploitation of Vulnerabilities (Zero-Day, Unpatched, Public-Facing)	Rapid weaponization of newly disclosed and existing flaws, especially in edge devices and internet-facing applications.	The most common initial infection vector (33%).[5] 25% of attacks exploit public-facing apps.[4] Zero-days weaponized within hours.[7] 40,000 new vulnerabilities in 2024 (39% increase).[8]	Immediate network compromise, privilege escalation, lateral movement, and data theft.
4. Sophisticated Ransomware and Extortion	Evolves beyond encryption to double extortion and business disruption. Adapts to reduced ransom payments by targeting vulnerable sectors.	28% of malware cases.[4] 86% of incidents led to operational downtime/reputational damage.[9] Decline in overall incidents but manufacturing remains highly targeted.[4]	Operational disruption, data exfiltration, financial loss, reputational damage.
5. Supply Chain Attacks	Targets third-party vendors and open-source components to infiltrate larger organizations.	Growing prominence in 2025.[7] Exploits trust and access granted to external entities.[7] Cloud environments and open-source ecosystems are key targets.[11]	Amplified impact across multiple organizations, widespread disruption, complex remediation.

The Evolving Cyber Threat Landscape in 2025

The cybersecurity landscape in 2025 is marked by unprecedented dynamism, primarily driven by the rapid advancements and weaponization of Artificial Intelligence (AI) by threat actors. This year, adversaries are demonstrating increased agility, leveraging automated tools and sophisticated techniques to bypass traditional defenses and achieve their objectives with greater speed and precision. The shift is not merely in the volume of attacks but in their complexity, targeting methodologies, and the convergence of multiple vectors to maximize impact. Leading reports from IBM X-Force, Mandiant, CrowdStrike, Fortinet, Palo Alto Networks, CSA, Beazley Security, and GovTech consistently highlight these shifts, emphasizing a critical need for organizations to move beyond reactive measures towards proactive, integrated, and resilience-focused security postures.

A significant development shaping this landscape is the role of AI as a universal amplifier of adversary capabilities. Threat actors are extensively employing AI, including generative AI (GenAI) and autonomous AI systems, to enhance their attack capabilities across the spectrum of cyber threats.[1] This includes using AI to construct malicious websites, integrate deepfakes into phishing campaigns, generate malicious code, automate reconnaissance, and create exploit scripts.[4] AI's ability to automate and scale operations means that attacks can be executed with greater speed and precision, often bypassing traditional security measures.[7] This fundamental transformation of attack methodologies means that traditional human-centric defense models are increasingly outpaced. The growing reliance on AI by attackers necessitates a corresponding adoption of AI-driven security solutions by defenders, leading to an escalating technological competition between the two sides. This dynamic environment demands continuous vigilance and innovation in security strategies to maintain an effective defense posture.

The 5 Most Common Cyber Attacks as of July 2025

The following five attack types represent the most prevalent and impactful threats organizations face in mid-2025, characterized by their evolving sophistication and widespread adoption by various threat actors.

1. AI-Enhanced Phishing, Social Engineering, and Automated Attacks

This category encompasses the pervasive use of artificial intelligence to create compelling and scalable deceptive campaigns, alongside the automation of various attack vectors, which significantly lowers the barrier to entry for cybercriminals. Threat actors are extensively leveraging AI to enhance their capabilities, including using generative AI to build malicious websites, incorporate deepfakes into phishing attacks, and write malicious code.[1]

Phishing remains a primary method for gaining access to sensitive information.By 2025, campaigns will be markedly more sophisticated, employing deepfake technology and advanced social engineering tactics to deceive even the most vigilant individuals.[7] AI-generated emails have demonstrated a significantly higher click-through rate, reaching 54%, compared to just 12% for human-composed emails, indicating their enhanced effectiveness.[1] This sophistication extends to voice phishing (vishing), with CrowdStrike reporting a staggering 442% increase in such attacks in the second half of 2024.[1] Deepfake technology, powered by AI, is becoming a formidable tool for fraud, misinformation, and cyber extortion, mimicking trusted figures to authorize financial transfers or disclose proprietary information.[7]

The proliferation of AI tools and Cybercrime-as-a-Service (CaaS) platforms means that advanced attack capabilities are no longer exclusive to highly skilled or nation-state actors.[3] This widespread availability of sophisticated tools significantly broadens the threat actor landscape, making it more challenging to predict and defend against attacks from a broader range of sources. Organizations must now assume a baseline of high sophistication from any attacker, regardless of their perceived skill level, as traditional defenses based on attacker profiling may become less effective.

Beyond direct financial or data theft, a core objective of these AI-enhanced attacks is to undermine trust within organizations and in external communications. Deepfakes, for instance, are used for misinformation and cyber extortion, specifically designed to cast doubt on security, trust in the media, and brand reputation.[7] AI-driven social engineering and phishing campaigns aim to deceive individuals by impersonating colleagues or executives to authorize fraudulent transactions.[7] This means cybersecurity defenses must explicitly account for authenticity verification mechanisms, not just data protection. This includes implementing multi-layered verification processes, robust user awareness programs, and potentially AI-driven disinformation security measures. The clever delivery and hiding of malware payloads further complicate detection, prolonging the time it takes to identify ransomware and data breaches.[4]

2. Identity-Based Attacks and Stolen Credentials

The compromise and misuse of legitimate user accounts and credentials have emerged as a dominant initial access vector, driven by infostealer malware and a thriving underground market for stolen access credentials. Identity-based attacks constituted 30% of total intrusions observed by IBM X-Force in 2024, marking the second consecutive year that attackers have adopted stealthy, persistent methods using valid accounts.[4] CrowdStrike also highlights the significant expansion of identity-based attacks.[1]

A key enabler for this trend is the proliferation of infostealer malware. The number of infostealers delivered via phishing emails increased by 84% year-over-year.[4] Mandiant's M-Trends 2025 report emphasizes the growing trend of infostealer malware being used to facilitate intrusions by leveraging stolen credentials.[6] Fortinet observed a staggering 500% increase in credential logs from systems compromised by infostealer malware on darknet forums, providing adversaries with ready-made access to corporate environments.[3] These stolen credentials form the backbone of ransomware and espionage operations.[3] Consequently, stolen credentials rose to become the second most common initial infection vector in 2024, accounting for 16% of intrusions and surpassing email phishing.[5]

The market for initial access has also seen an explosion, with access broker advertisements touting available access to compromised environments surging by 50% in 2024.[1] Fortinet noted a 42% increase in compromised credentials available for

sale, alongside a surge in Initial Access Broker (IAB) activity offering VPNs, RDPs, and admin panels.[3]

A significant portion of these attacks are malware-free, relying on "hands-on-keyboard" activities. In 2024, 79% of detections tracked by CrowdStrike did not include malware, suggesting attackers are carrying out manual activities that mimic legitimate user behavior, making them harder to detect.[1] This allows adversaries to "live off the land," leveraging legitimate tools and protocols for privilege escalation and persistence.[3] The shift to malware-free, legitimate-tool-based attacks, combined with longer dwell times, means attackers are not just "breaking in" but "logging in" and operating as legitimate users. This makes detection incredibly difficult, allowing for prolonged reconnaissance and data exfiltration, and increasing the potential for significant business disruption and data theft over extended periods. Consequently, organizations require advanced behavioral analytics, continuous monitoring, and anomaly detection to identify subtle deviations from normal user behavior.[15]

The increasing reliance on cloud environments means that identities have become the new perimeter. Compromised credentials directly translate into unauthorized access to cloud resources, bypassing traditional network defenses. This makes Identity and Access Management (IAM) a critical control point for cloud security. Security strategies must therefore shift from perimeter-centric to identity-centric, especially in hybrid and cloud environments, with strong IAM practices, including multi-factor authentication (MFA) and least privilege access, being paramount.[15]

3. Exploitation of Vulnerabilities (Zero-Day, Unpatched, Public-Facing)

The rapid weaponization of newly disclosed and existing vulnerabilities, particularly in internet-exposed applications and edge devices, remains a critical and frequently exploited initial access vector. Exploits were the most common initial infection vector in Mandiant's investigations in 2024, accounting for 33% of intrusions where a vector was identified.[5] CrowdStrike also noted that 52% of observed vulnerabilities were related to initial access, underscoring their importance in gaining initial footholds.[2]

Zero-day vulnerabilities continue to pose a significant risk, particularly for internet-exposed edge devices, including VPNs and firewalls.[7] The speed at which these vulnerabilities are exploited is alarming, with cybercriminals weaponizing them within hours of discovery.[7] IBM X-Force reported that four out of the top 10

vulnerabilities mentioned on the dark web are linked to sophisticated threat actors, with 60% being actively exploited or having publicly available exploits within two weeks of disclosure or as zero days.[4] One in four attacks (25%) exploited vulnerabilities in common public-facing or internet-accessible applications, with threat actors using active scanning post-compromise to identify new vulnerabilities and move laterally.Mandiant highlighted that the most frequently exploited vulnerabilities affected security devices, often at the network edge, with examples including vulnerabilities in Palo Alto Networks PAN-OS, GlobalProtect, and Ivanti Connect Secure VPN.[6] The sheer volume of new vulnerabilities is also a challenge, with over 40,000 new vulnerabilities added to the National Vulnerability Database in 2024, a 39% increase from 2023.[8]

Despite increased awareness and vulnerability disclosures, organizations often struggle to patch quickly enough to close the window of opportunity for attackers. This "patch gap" or "exploit window" is a persistent and critical strategic weakness, particularly for internet-exposed devices that represent high-value targets. The sheer volume of new vulnerabilities exacerbates this challenge, making comprehensive and timely patching a formidable task. This situation emphasizes that prioritizing patch management, enhancing monitoring for unauthorized access, and implementing continuous threat exposure management are no longer optional but fundamental to an organization's security posture.[3] Focus should be placed on high-risk vulnerabilities actively discussed in cybercrime forums.[8]

The dark web plays a crucial role in accelerating the exploitation cycle. Top vulnerabilities are frequently discussed and traded on the dark web.[4] Sophisticated threat actors leverage the anonymity of the dark web to acquire new tools and resources.[4] Darknet forums function as marketplaces for exploit kits and initial access services, making exploits widely available to a broader range of threat actors, including those who may lack the capability to develop them independently.[8] This underscores the importance for organizations to monitor dark web intelligence to detect emerging threats and prioritize remediation efforts based on vulnerabilities actively discussed and traded in these underground communities.[8]

4. Sophisticated Ransomware and Extortion

While overall ransomware incidents have seen a decline, the nature of these attacks has evolved, with cybercriminals employing more advanced techniques like double

extortion and shifting their focus towards business disruption rather than just data encryption. Ransomware continues to be a prevalent and damaging attack.[10] In 2025, there is an anticipated surge in sophisticated operations, particularly targeting critical infrastructure, healthcare systems, and financial institutions.[10]

Cybercriminals are increasingly employing double extortion, where they not only encrypt data but also threaten to release sensitive information if a ransom is not paid.[10] Forrester notes that generative AI now enables attackers to quickly perform sentiment analysis on troves of stolen data for more effective extortion schemes, making the threat of data-driven extortion more potent.[13] Palo Alto Networks' Unit 42 report indicates that threat actors are moving beyond traditional ransomware and data theft to focus on business disruption, with 86% of incidents in 2024 leading to operational downtime or reputational damage.[9]

IBM X-Force observed a decline in ransomware incidents overall in 2024, marking the third consecutive year of decline, possibly due to businesses being more reluctant to pay ransoms and increased government actions against ransomware groups.[4] However, ransomware still constituted 28% of malware cases.[4] Despite the overall decline, the manufacturing industry experienced the highest number of ransomware cases in 2024, as attackers continue to exploit outdated legacy technology in this sector.[4] This indicates that ransomware operators are not disappearing but are strategically adapting to changing market conditions. This adaptation involves targeting more vulnerable sectors where they can still find success and shifting their leverage from mere encryption to a broader spectrum of disruption and data-driven extortion. This suggests a more strategic and less opportunistic approach to ransomware. Organizations must therefore prepare for more targeted, sophisticated, and disruptive attacks that leverage multiple forms of coercion, emphasizing the paramount importance of business resilience and robust data backup and recovery plans.[10]

The Ransomware-as-a-Service (RaaS) ecosystem continues to evolve. While 13 new RaaS groups emerged in 2024, suggesting market fragmentation, the top four groups still accounted for 37% of observed attacks, underscoring their continued dominance.[3] Hacktivists are also increasingly adopting ransomware tactics.[3] Furthermore, cybercriminals are preparing for post-quantum cryptography by adapting ransomware capabilities for future resilience.[11]

A critical aspect of modern ransomware and extortion operations is their reliance on initial access gained through infostealers and compromised credentials. Infostealers are fueling identity-based attacks and stolen credentials, which have become primary

initial access vectors.[3] These stolen credentials form the "backbone of ransomware and espionage operations".The rise of generative AI-driven extortion, which leverages stolen data, is becoming a more significant threat than traditional ransomware.[14] This indicates that info stealers are not just a separate threat but a foundational enabler for modern ransomware and extortion. By providing valid credentials, infostealers bypass initial defenses, allowing ransomware groups to gain stealthy access and then pivot to encryption or, increasingly, data exfiltration for double extortion. Therefore, defenses against ransomware must extend far upstream to aggressively counter info stealers and credential theft, including strong authentication (MFA), endpoint protection, and proactive monitoring for compromised credentials.

5. Supply Chain Attacks

The increasing complexity and interconnectivity of modern supply chains make third-party vendors and suppliers attractive targets for cybercriminals seeking to infiltrate larger organizations and achieve widespread impact. Supply chain attacks have gained prominence in recent years and are expected to continue this trend in 2025.[7]

Attackers specifically target third-party vendors and suppliers to infiltrate larger organizations by exploiting the trust and access granted to these external entities.[7] This method not only amplifies the impact of a breach but also challenges organizations to secure not just their infrastructure but also that of their partners.Seven cloud environments are key targets, as attackers exploit weak links in complex cloud supply chains.[11] Mandiant emphasizes that continuous monitoring of supply chain security is necessary due to these risks.[15] Additionally, cybercriminals are targeting open-source ecosystems, exploiting code dependencies to disrupt organizations.[11]

Organizations often have an implicit "trust blind spot" when it comes to third-party vendors, assuming their security posture is adequate. However, the interconnected nature of modern business, especially with the widespread adoption of cloud services and open-source dependencies, means that a compromise in one trusted entity can cascade through the entire supply chain. This makes the weakest link in the chain a critical vulnerability for all connected entities. Consequently, comprehensive security assessments of suppliers, stringent access controls for third parties, and continuous monitoring of third-party activities are no longer optional but fundamental to an

organization's security.[7] This necessitates a strategic shift towards prioritizing "vendor resilience" as a core component of overall cybersecurity.[11]

Supply chain attacks are not solely driven by financially motivated cybercrime; they are increasingly a vectors for nation-state espionage and strategic disruption. Nation-state actors are becoming more sophisticated and frequently target key industries.[10] China-nexus adversaries, for example, are aggressively targeting manufacturing, financial services, and critical infrastructure, often through supply chains.[1] Geopolitical cyber warfare is intensifying, with prominent state-sponsored actors aligning their campaigns with geopolitical interests.[11] Targeting critical infrastructure through supply chains can have cascading impacts on national economies and security.[16] This elevates supply chain risk from a purely technical problem to a geopolitical one. Organizations, especially those in critical sectors or with ties to global supply chains, must consider the geopolitical context of their vendors and partners. This may necessitate deeper due diligence, diversification of suppliers, and proactive collaboration with government agencies for threat intelligence.[10]

Cross-Cutting Trends and Implications

Beyond the specific attack types, several overarching trends are reshaping the cybersecurity landscape in 2025, demanding a fundamental shift in defensive strategies.

The pervasive role of AI in both offensive and defensive cybersecurity is undeniable. As detailed previously, AI is a game-changer for attackers, enabling the automation, scaling, and sophistication of attacks across various vectors.[1] Concurrently, organizations are increasingly adopting AI-driven security solutions to counter these threats, with AI-powered Security Operations Centers (SOCs) improving threat detection and automating incident response.Gartner predicts that AI will be tactically integrated into security programs to deliver measurable benefits.[17] This creates a continuous technological competition, where both sides leverage AI, demanding continuous vigilance and innovation in security strategies. The success of defensive AI heavily relies on access to vast, high-quality data for training and refining models.[12]

Another significant trend is the shift towards malware-free and "hands-on-keyboard" attacks. A substantial proportion of attacks now forgo traditional malware, instead relying on compromised credentials and manual activities to mimic legitimate users.[1] This approach renders traditional signature-based detection less effective, as there are no malicious files to scan for. Organizations must therefore pivot their defenses to focus on behavioral analytics, anomaly detection, and continuous monitoring of user and system activities to identify subtle indicators of compromise that might signal an adversary "living off the land".[15]

The increasing targeting of cloud environments presents unique challenges. Cloud environments remain a top target, with new and unattributed cloud intrusions on the rise.[2] Common vulnerabilities stem from misconfigurations, open storage buckets, and over-permissioned identities.[8] Valid account abuse is a primary initial access tactic in cloud incidents.[2] This indicates that cloud security is no longer solely about infrastructure protection; it fundamentally involves identity management, rigorous configuration management, and continuous monitoring across complex multi-cloud environments. Traditional incident response plans often fail to account for cloud complexity [15], necessitating new approaches and the adoption of unified security platforms that can provide holistic visibility.[12]

A paradoxical trend in the current threat landscape involves both the acceleration of

attack speeds and the persistence of long dwell times. Breakout times, which measure the duration from initial compromise to lateral movement, are hitting record speeds, with the average eCrime breakout time decreasing to 48 minutes and the fastest recorded at a mere 51 seconds.[2] Attackers are also exfiltrating data three times faster than in 2021.[9] Conversely, the global median dwell time—the duration an attacker is present before detection—increased to 11 days in 2024.[6] This seemingly contradictory observation points to a sophisticated adversary strategy: attackers are capable of rapid initial strikes when opportunities arise (e.g., zero-day exploitation, valid credentials), but once inside, they prioritize stealth and persistence. This allows them to remain undetected for extended periods, enabling deeper reconnaissance and more impactful data exfiltration or disruption. This combination of rapid initial compromise and potentially long dwell times creates a challenging environment for defenders, leaving little room for error in initial detection and response. This emphasizes the need for real-time threat intelligence, automated response mechanisms, and a strategic shift from prevention-only to a resilience-focused mindset.[17]

The increasing complexity of attacks, with 70% of incidents involving three or more attack vectors, highlights the inadequacy of siloed security tools.[9] Fragmented security systems create blind spots, slowing down detection and response efforts.[12] The imperative for effective defense is, therefore, integration. A unified platform that integrates data from endpoints, networks, cloud environments, and identity systems allows for comprehensive visibility and AI-powered analysis across the entire attack surface, enabling faster detection and response. Organizations must prioritize vendor and tool consolidation, focusing on integrated security platforms that provide holistic visibility and enable AI-driven automation. This approach is crucial for significantly reducing Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) to minutes.[12]

Conclusion

The cybersecurity landscape in July 2025 is defined by a dynamic and increasingly sophisticated threat environment. The five most common attack types—AI-enhanced phishing and social engineering, identity-based attacks, rapid exploitation of vulnerabilities, sophisticated ransomware and extortion, and pervasive supply chain attacks—are not isolated incidents but interconnected facets of a broader, industrialized cybercrime ecosystem. The pervasive influence of AI, the shift towards stealthy, malware-free intrusions, the persistent targeting of cloud environments, and the paradoxical trends in attack speed and dwell time underscore the urgent need for adaptive and proactive security measures.

To effectively navigate this evolving landscape, organizations must prioritize integrated, AI-driven security platforms that offer comprehensive visibility across their entire digital estate. Robust identity and access management, including multi-factor authentication and least privilege principles, is paramount as identities increasingly serve as the new security perimeter. Continuous threat exposure management, focusing on rapid patching of high-risk vulnerabilities and proactive monitoring for anomalous behaviors, is essential to minimize the window of opportunity for attackers. Furthermore, comprehensive supply chain risk assessments, extending to geopolitical considerations, are critical to mitigate the risks posed by interconnected ecosystems. By embracing these principles and fostering a culture of resilience, businesses can significantly enhance their ability to detect, respond to, and recover from sophisticated cyber attacks, thereby securing their digital future.

Works Cited:

1. Five Big Takeaways From CrowdStrike's 2025 Threat Report - CRN, accessed July 5, 2025, https://www.crn.com/news/security/2025/five-big-takeaways-from-crowdstrike-s-2025-threat-report
2. CrowdStrike Releases 2025 Global Threat Report: Cyber Threats ..., accessed July 5, 2025, https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-global-threat-report/
3. Fortinet FortiGuard Labs 2025 reports cybercrime-as-a-service ..., accessed July 5, 2025, https://industrialcyber.co/reports/fortinet-fortiguard-labs-2025-reports-cybercrime-as-a-service-boom-as-hackers-weaponize-ai-amid-industrialized-threat-surge/
4. IBM X-Force 2025 Threat Intelligence Index | IBM, accessed July 5, 2025, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
5. Mandiant Releases Annual M-Trends Report - Cyber Risk Leaders, accessed July 5, 2025, https://cyberriskleaders.com/mandiant-releases-annual-m-trends-report/
6. M-Trends 2025 Report - Google Services, accessed July 5, 2025, https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
7. Top Five Predicted Cyber Threats for 2025 - Beazley Security, accessed July 5, 2025, https://beazley.security/insights/top-five-predicted-cyber-threats-for-2025
8. Fortinet 2025 Threat Report: AI-Driven Cyberattacks Surge 500 ..., accessed July 5, 2025, https://www.dqchannels.com/news/fortinet-releases-2025-global-threat-landscape-report-cyberattack-trends-9035659
9. 2025 Unit 42 Global Incident Response Report Reveals Nearly 44 ..., accessed July 5, 2025, https://cybersecurityasia.net/2025-unit-42-global-incident-response-report/
10. What Are the Top Cybersecurity Threats of 2025? | CSA, accessed July 5, 2025, https://cloudsecurityalliance.org/blog/2025/01/14/the-emerging-cybersecurity-threats-in-2025-what-you-can-do-to-stay-ahead
11. The Top 25 Security Predictions for 2025 (Part 1) - GovTech, accessed July 5, 2025, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-25-security-predictions-for-2025-part-1
12. 2025 Cybersecurity Predictions - Palo Alto Networks, accessed July 5, 2025, https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
13. The Top Cybersecurity Threats In 2025 | Forrester, accessed July 5, 2025, https://www.forrester.com/webinar/The+Top+Cybersecurity+Threats+In+2025/WEB40617
14. Forrester's Top Threats For 2025, accessed July 5, 2025, https://www.forrester.com/blogs/forresters-top-threats-for-2025/
15. Top Threats 2025 | 8 Real-World Cybersecurity Breaches | CSA, accessed July 5, 2025, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025
16. Homeland Threat Assessment 2025, accessed July 5, 2025, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf
17. Key Trends from Gartner® Cybersecurity Research | Rapid7 Blog, accessed July 5, 2025, https://www.rapid7.com/blog/post/2025/05/01/ai-and-resilience-take-the-spotlight-in-2025-key-trends-from-gartner-r-cybersecurity-research/