

2025 Global Threat Analysis Report

Analysis of the Global Network and
Application Attack Trends of 2024

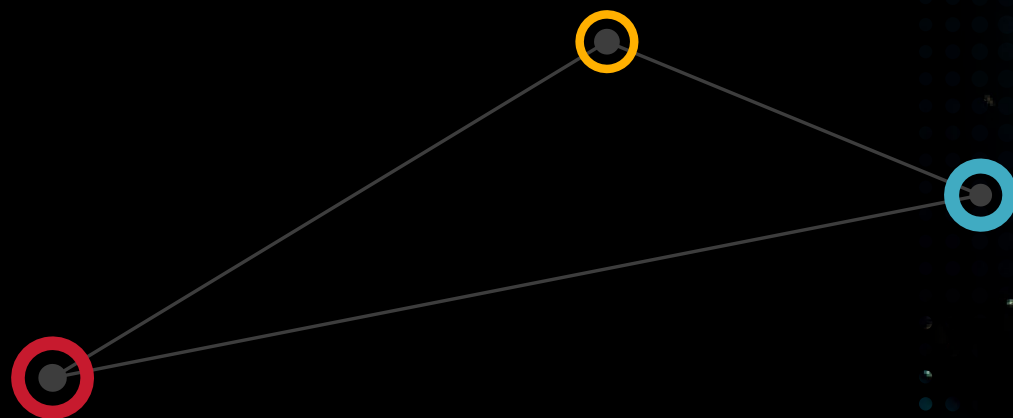
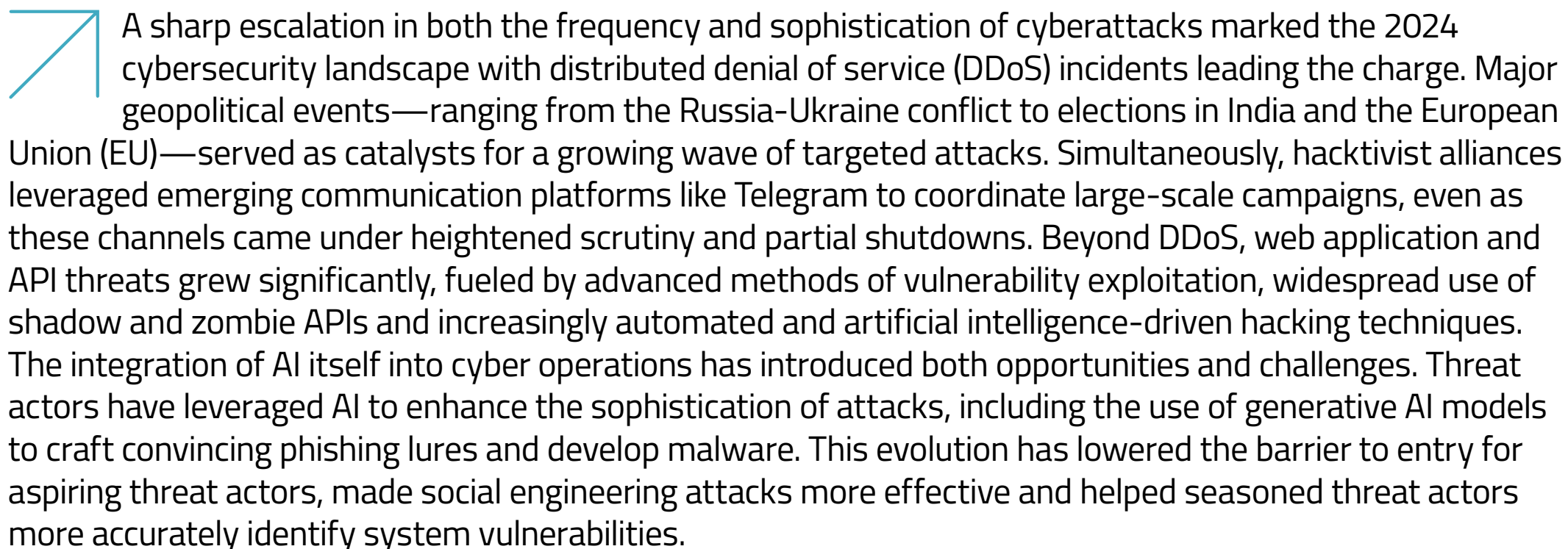


Table of Contents

| | |
|--|-----------|
| Executive Summary | 3 |
| The DDoS Threat Landscape | 4 |
| Escalation of Web DDoS Attacks | 4 |
| Network DDoS Evolution | 4 |
| DDoS-for-hire Services | 4 |
| Hacktivism and Alliances | 5 |
| Hacktivist Motivations and Targets | 5 |
| Alliances and Collaboration | 5 |
| The Role of Telegram | 5 |
| Web Application and API Threats | 6 |
| Rapid Expansion of Attacks | 6 |
| Surge in API Exploitation | 6 |
| Shadow and Zombie APIs | 6 |
| Advanced Attack Techniques | 6 |
| The Bad Bot Threat | 7 |
| Growing Proportions and Sophistication | 7 |
| AI-Driven and “Grey” Bots | 7 |
| AI in Cybercrime | 8 |
| Advanced Phishing and Deepfakes | 8 |
| AI-Enhanced Attacks | 8 |
| Offline AI Models: The New Frontier in Cyberattacks | 8 |
| Lowering the Barrier to Entry for New Cybercriminals | 8 |
| Direct Attacks on AI Systems | 8 |
| Conclusion | 9 |
| About Radware | 10 |



Executive Summary



A sharp escalation in both the frequency and sophistication of cyberattacks marked the 2024 cybersecurity landscape with distributed denial of service (DDoS) incidents leading the charge. Major geopolitical events—ranging from the Russia-Ukraine conflict to elections in India and the European Union (EU)—served as catalysts for a growing wave of targeted attacks. Simultaneously, hacktivist alliances leveraged emerging communication platforms like Telegram to coordinate large-scale campaigns, even as these channels came under heightened scrutiny and partial shutdowns. Beyond DDoS, web application and API threats grew significantly, fueled by advanced methods of vulnerability exploitation, widespread use of shadow and zombie APIs and increasingly automated and artificial intelligence-driven hacking techniques. The integration of AI itself into cyber operations has introduced both opportunities and challenges. Threat actors have leveraged AI to enhance the sophistication of attacks, including the use of generative AI models to craft convincing phishing lures and develop malware. This evolution has lowered the barrier to entry for aspiring threat actors, made social engineering attacks more effective and helped seasoned threat actors more accurately identify system vulnerabilities.



The DDoS Threat Landscape

Escalation of Web DDoS Attacks

Web DDoS attacks escalated significantly, increasing almost 550% year-over-year compared to 2023. The intensity of these attacks grew exponentially during the first half of the year and plateaued at high levels during the second half, reflecting a sustained and aggressive threat environment. Use of advanced Layer 7 (L7) DDoS attacks became a prominent tactic, leveraging vulnerabilities such as the HTTP/2 Rapid Reset and Continuation Flood to target online applications with increasing sophistication. Notable incidents included a six-day attack on a financial institution in the Middle East, which peaked at 14.7 million requests per second (RPS), and another attack on a major institution that reached 16 million RPS.

Europe, the Middle East, and Africa (EMEA) remained the primary target for Web DDoS attacks, accounting for 78% of global incidents. Political tensions such as the Russia-Ukraine conflict, combined with EU elections and various international sporting events, provided ample impetus for threat actors to strike at high-value targets. Elsewhere, Asia-Pacific (APAC) saw DDoS activity climb to 8% of the global total.

Network DDoS Evolution

Network DDoS attacks in 2024 witnessed significant upticks in intensity and duration. The average mitigated attack volume per customer doubled compared to 2023, contributing to an overall 120% rise in total volume. The average duration continued to grow considerably in 2024 with a 37% increase over 2023. The average attack frequency, volume and duration have all more than doubled since 2022.

“Low and slow” attack strategies, designed to evade detection, increased by 38% and lasted an average duration of 9.7 hours in 2024, more than doubling the average duration of 4.6 hours in 2023.

The year 2024 witnessed an unprecedented amount of DNS query flood denial of service attacks, which surpassed the previous year by 87%. This marked 2024 as another pivotal year in the evolution of cyberthreats and, more specifically, L7 DNS DoS attacks. The financial sector bore the brunt of this continued evolution, accounting for 44% of the total L7 DNS attack activity. Other significantly affected sectors included healthcare (13%) and telecom (10%).

UDP and DNS amplification attacks continued to dominate volumetric DDoS methods with DNS amplification alone accounting for 65% of all amplification-based attacks.

Organizations in Europe faced the highest proportion of network DDoS activity, accounting for 44.5% of the global attack volume and 32.5% of the total malicious packets. North American organizations were the second most targeted by volume, experiencing 21% of global attack traffic. The Middle East ranked as the second most targeted by packets, intercepting 24% of global malicious packets. Organizations in Oceania faced the highest average network DDoS volume and packet counts per customer.

Telecommunications faced 43% of global network DDoS volume. Finance followed at 30%, experiencing the steepest growth in attack volume per customer at 393% year-over-year—more than twice the global average growth of 120%. Technology absorbed 11% of the global network DDoS attack volume, while transportation, e-commerce and government services also observed notable surges.

The United States emerged as both the leading attacker and target of network-layer traffic, reflecting a potentially significant DDoS resource presence and the attractiveness of U.S. assets to global adversaries. For both top attacking and most targeted countries, United States and Israel, the majority of the attack volume originated from infrastructure and bots inside the country. While the threat from inside the country is significant, still 12% of all malicious network DDoS packets were mitigated by geo-blocking.

DDoS-for-hire Services

The rise of DDoS-for-hire platforms has further democratized access to potent offensive capabilities, lowering the technical threshold required to launch large-scale attacks. These services have contributed to an increase in application-layer DDoS assaults, which are generally more challenging to detect and mitigate than network-layer attacks.

Hacktivism and Alliances

Hacktivist Motivations and Targets

Throughout 2024, hacktivism remained a leading driver of cyberattacks, propelled by political and ideological tensions. The total number of claimed DDoS attacks on Telegram increased by 20% compared to 2023. Ukraine topped the list of targeted nations, with 2,052 claimed attacks, predominantly orchestrated by pro-Russian groups such as NoName057(16), which boasted 4,767 claims. High-profile events like India's national elections in June sparked further activity, as cyber vigilantes on both sides used DDoS and data exfiltration attacks to advance political agendas.

Government institutions remained the primary target of attacks since January 2023, representing 20% of hacktivist activity in 2024. E-commerce platforms and organizational websites were also heavily targeted (9%), as well as the financial sector (8.9%) and other industries including transportation (7%), media and internet (7%), and manufacturing (6.9%). NoName057(16) consistently emerged as the primary threat actor across all the most targeted sectors.

Alliances and Collaboration

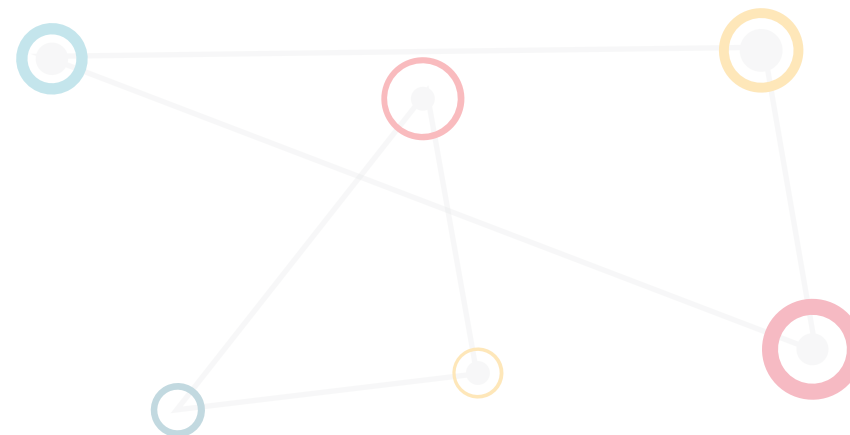
Despite historically operating as "lone wolves," even groups like NoName057(16) have begun forming strategic alliances. Notably, pro-Russian and pro-Palestinian hacktivists joined forces in coordinated campaigns to strike common perceived adversaries. These alliances boosted operational capabilities, often resulting in multi-vector attacks that fused techniques and resources from multiple collectives.

The Role of Telegram

In 2024, Telegram acted as a primary coordination and communication hub for hacktivist groups, largely due to its anonymity features and lenient moderation. Following the arrest of its founder and CEO, Pavel Durov, in August 2024, Telegram increased its cooperation with law enforcement and stepped up moderation efforts, as evidenced by a surge in data-sharing with authorities. For instance, it [fulfilled 900 U.S. government requests](#) in the latter half of 2024. Concurrently, the European Union restricted certain Telegram channels deemed to violate EU laws, including Russian state-owned news and hacktivist channels like the Pro-Palestinian Hacker Movement (PPHM).

Despite the heightened scrutiny, Telegram remains vital for hacktivist operations. Some prominent channels—such as those of NoName057(16) and CARR (Cyber Army of Russia Reborn)—were banned, not through official moderation but seemingly via ban-spamming attacks from rival groups.

Meanwhile, Telegram's bot automation and cryptocurrency services have encouraged the rise of DDoS-as-a-service offerings, letting individuals hire attacks through Telegram bots that handle real-time commands, scheduling and payments. This ecosystem has made it alarmingly easy for users with minimal technical skills to launch or commission DDoS attacks, further cementing Telegram's role in the global hacktivist and cybercriminal landscape.



Web Application and API Threats

Rapid Expansion of Attacks

In 2024, the rise of Web application and API attacks continued, increasing 41% over 2023. Vulnerability exploitation remained the most prominent attack type, comprising one-third of all malicious requests. North America experienced 66% of these attacks, followed by EMEA at 26%, highlighting a strong concentration of targeted applications in developed markets.

Surge in API Exploitation

Because of their broad adoption, APIs now represent a substantial portion of online web application traffic and have become prime targets. Their inherently automated nature—which requires no human intervention—makes them especially vulnerable to automated assaults. Threat actors increasingly exploit this vulnerability to compromise the business logic or core functionality of APIs. By emulating legitimate automated API requests, these attacks often go unnoticed, allowing malicious actors to operate without disruption.

Shadow and Zombie APIs

The rapid pace of development and innovation in online applications has given rise to numerous APIs that either lack proper documentation (shadow APIs) or are outdated and no longer actively maintained (zombie APIs). These unmanaged and often overlooked endpoints serve as enticing entry points for unauthorized access, significantly increasing the risk of data breaches. For security teams, these neglected APIs create critical blind spots, undermining their ability to maintain a comprehensive defense. Cybercriminals are increasingly exploiting these vulnerabilities, using shadow and zombie APIs to establish an initial foothold in systems or to stealthily exfiltrate sensitive information, often remaining undetected for extended periods. As a result, these hidden gateways have become high-priority targets in the evolving threat landscape.

Advanced Attack Techniques

Business logic vulnerabilities have already found their place among the [OWASP Top Ten API Security Risks](#) and they are among the [HackerOne Top Ten Vulnerability Types](#), which is based on bug bounty reports. Cybercriminals continually advance their tactics while researchers demonstrate practical use cases for emerging attack methodologies such as [web timing attacks](#).



The Bad Bot Threat

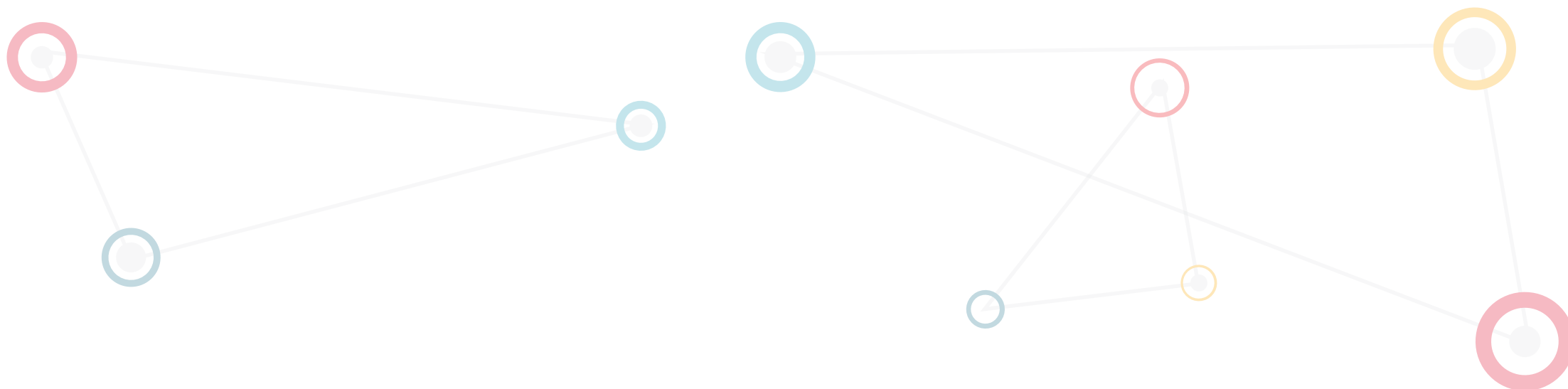
Growing Proportions and Sophistication

Bad bot activity grew significantly in 2024, with a 35% increase in malicious transactions compared to 2023, following a 26% rise in 2023 relative to 2022. Bad bot activity is consistently higher in the second half of the year, an observation that aligns with high-traffic periods such as Black Friday, Cyber Monday and the winter holiday season when promotional campaigns and increased online activity make platforms more susceptible to such transactions.

Bad bots, responsible for activities such as account takeover, fraud and web scraping, made up 71% of all bot traffic in 2024. North America emerged as the most targeted region, accounting for half of all bad bot transactions, while EMEA, APAC and CALA regions experienced lower but still notable levels of activity.

AI-Driven and “Grey” Bots

The surge in AI technologies gave rise to sophisticated “grey” bots, which aggressively scrape data to train AI models—often without explicit permission. AI is also rapidly becoming the next major focus for search engine optimization (SEO) strategies. With the rise of AI-driven tools like generative AI models, conversational AI and AI-powered search engines, the SEO landscape is evolving to prioritize content that aligns with AI processing and user behavior in AI-assisted searches. This adds a layer of ethical and operational complexity, as data owners grapple with how to protect their assets without hindering legitimate AI scrapers used for research and for SEO.



AI in Cybercrime

Advanced Phishing and Deepfakes

Cybercriminals utilized AI to generate highly persuasive phishing emails, text messages and even deepfake videos. This level of realism severely impedes an organization's ability to distinguish authentic communications from fraudulent ones. As the World Economic Forum warned, the prevalence of AI-driven social engineering demands robust awareness training and multi-layered defenses.

AI-Enhanced Attacks

Studies in 2024 showcased the potential for adaptive and self-learning capabilities in AI agents, enabling them to select the most promising exploits. By integrating AI, attackers can continuously test defenses, identify weaknesses, and generate and deploy customized payloads at unprecedented speed.

Offline AI Models: The New Frontier in Cyberattacks

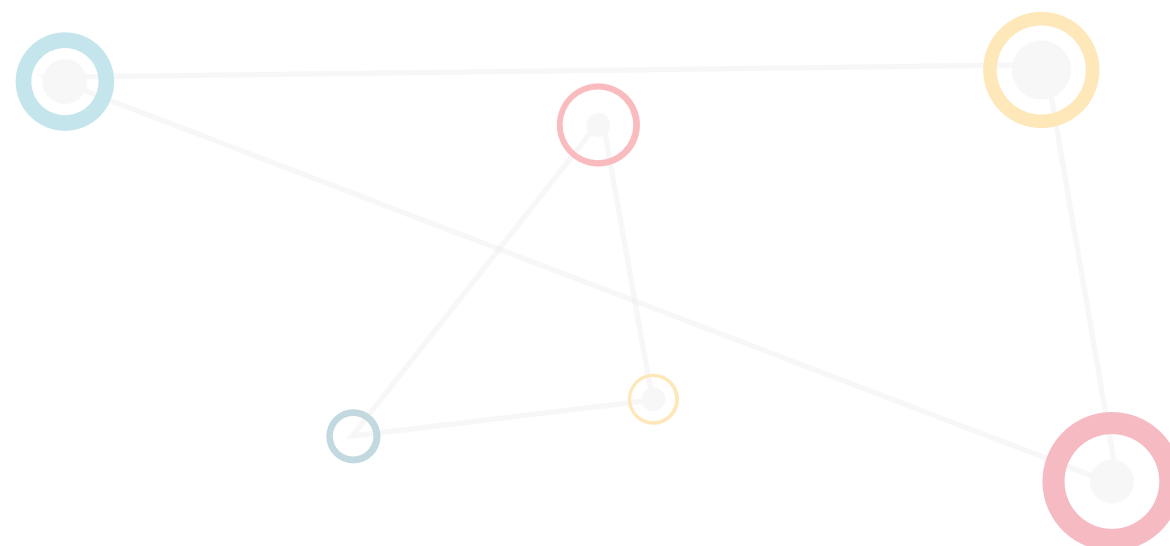
The advent of downloadable, pre-trained AI models has transformed the cybersecurity landscape, enabling broader adoption and innovation in both defense and offense. Unlike traditional neural networks requiring significant resources, offline models are accessible and modifiable, presenting new security risks. While cloud-based AI systems maintain ethical safeguards, offline models can be exploited for malicious purposes. Tools like WormGPT and FraudGPT can be used to enhance malware or automate phishing campaigns. This underscores the ongoing technological race between cyber defenders and threat actors, as the potential for fully automated attack campaigns looms on the horizon.

Lowering the Barrier to Entry for New Cybercriminals


AI-based hacking resources became more accessible in 2024, lowering the barrier to entry for potential cybercriminals. A [Bugcrowd study](#) revealed that 71% of hackers felt AI boosted the "value" of hacking, up from 21% in 2023, while 77% reported using generative AI tools—up from 64% the previous year.

Direct Attacks on AI Systems

AI platforms themselves are high-value targets. By manipulating training data or forcing AI systems into unexpected behaviors, attackers can degrade service reliability or generate flawed outputs, raising concerns about data integrity and brand reputation.



Conclusion



The year 2024 underscored a clear trajectory: cyberthreats are not only proliferating but becoming more adept at circumventing traditional defenses. From massive volumetric DDoS campaigns to Layer 7 attacks that exploit newly discovered vulnerabilities, the scope of DDoS alone has expanded far beyond the capability of older, static protections. Concurrently, hacktivist collectives showcased unprecedented levels of coordination, while web application and API threats continued to multiply under the weight of complex infrastructures and widespread reliance on third-party components. Bad bots and AI-powered cybercrime have redefined what is possible in terms of evasion, automation and destructive potential.

With these developments come significant implications for every sector: finance, telecommunications, government, e-commerce and beyond. The confluence of political motivations, advanced technology and criminal innovation creates a dynamic threat environment that demands equally dynamic defense strategies. Organizations must not only adopt layered protection strategies but also invest in ongoing risk assessments, cyberthreat intelligence and employee education to stay one step ahead of adversaries. By recognizing and preparing for the realities of 2024's threat landscape, stakeholders can better safeguard their operations, assets and reputations in the years to come.



Read the complete
2025 Global Threat Analysis Report.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILABILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.

