RAPID7

EXECUTIVE BRIEF

DECODING THE ACCELERATED CYBER ATTACK CYCLE

A CISO briefing on the Rapid7 2026 Global Threat Landscape Report

Executive perspective: Speed is no longer your advantage

Security did not fail in 2025 because defenders were slow. It failed because speed stopped being a differentiator.

The defining feature of this year's threat data is acceleration. Attackers are not relying on radically new techniques, they are executing known playbooks faster, at scale, and with tighter operational discipline. Automation, artificial intelligence (AI), and the industrialization of the cybercrime ecosystem have compressed the time between exposure and impact. What once took weeks now takes days — sometimes minutes.

For CISOs, this shifts the operating model. The central question is no longer how fast you can respond, but how well you can reduce your exposure before attackers exploit it.

1. THE PREDICTIVE WINDOW HAS COLLAPSED

The most consequential shift in 2025 is this: the predictive window has collapsed. Confirmed exploitation of newly disclosed **CVSS 7–10 vulnerabilities increased 105%** year over year, from **71 in 2024 to 146 in 2025.** Over four years, exploited vulnerabilities grew from 7 in 2022 to 146 in 2025, and the exploitation rate relative to disclosure volume rose from less than 0.1% to 0.8%.

Timing compressed as well. Median time from publication to CISA Known Exploited Vulnerabilities (KEV) inclusion dropped from 8.5 days to 5.0 days, and the mean fell from 61.0 days to 28.5 days. Meanwhile, the "high-risk but not yet exploited" category largely disappeared. In 2024, 338 vulnerabilities had an exploit prediction scoring system (EPSS) score ≥ 0.7 without confirmed exploitation; in 2025, only 65 remained. Within the Emerging Threat Response dataset, high-risk-but-unexploited vulnerabilities fell from **15 to 1**, while confirmed exploitation rose from 5 to 22.

High-impact vulnerabilities are now operational assumptions, not probabilities. Traditional prioritization cycles are misaligned with attacker timelines. In 2025, SOCs were not overwhelmed by volume. They were outpaced by velocity.

2. ATTACKERS ARE MONETIZING UNMANAGED EXPOSURE

Most intrusions in 2025 began with preventable exposures, not novel zero-days. Valid accounts without **multi-factor authentication accounted for 43.9% of incidents**. Vulnerability exploitation represented 24.6%, and exposed services 7.0%.

Underground marketplace activity reflects the same pattern. **Remote Desktop Protocol access accounted for 21.2% of listings, VPN access 12.8%, and RDWeb 11.2%**. Domain-level privileges were commonly offered, and access was routinely packaged and sold. In just six months, DarkForums listed 221 access offerings and RAMP listed 208. The average alleged revenue of victim organizations exceeded $3.2 billion, with an average base price of $113,275 per listing. Initial access brokers have industrialized exposure. They harvest credentials, validate access, and sell it as inventory acting in ways that legitimate businesses would.

3. EXPLOITATION IS CONCENTRATING ON RELIABLE WEAKNESS CLASSES

Although total high and critical CVEs rose moderately from approximately 16,200 to 18,100 year over year, exploitation did not scale evenly. It clustered around a narrow set of reliable weakness classes.

CWE-502 (deserialization) was the most commonly exploited root cause in 2025, with authentication bypass and memory corruption consistently represented. High-profile ransomware campaigns targeted deserialization flaws and authentication bypass in file transfer systems, collaboration platforms, and edge appliances.

By contrast, high-volume disclosures such as cross-site scripting and SQL injection were far less prominent in confirmed exploitation. Attackers are prioritizing reliability, pre-authentication access, and scalable remote code execution.

For vulnerability management programs, this underscores the need to prioritize based on exploitability, asset role, and exposure context rather than raw CVE counts.

4. RANSOMWARE HAS MATURED INTO A SPEED-OPTIMIZED ACCESS ECONOMY

Ransomware remained a dominant operational outcome in 2025, **accounting for 42% of Rapid7 MDR investigations**. Leak posts increased from 6,034 in 2024 to 8,835 in 2025, a **46.4%** rise. Unique active ransomware groups grew from 102 to 140, and average posts per group also increased.

Qilin led leak posts with 1,029 entries, followed by Akira and Cl0p. Double extortion and ransomware-as-a-service models dominated the ecosystem. Data theft frequently preceded encryption, reflecting smash-and-grab extortion tactics designed to maximize leverage quickly.

Importantly, ransomware incidents overwhelmingly originated from predictable pathways such as compromised credentials, exposed VPN or RDP services, and unpatched edge infrastructure. This is not simply a ransomware problem, it is the monetization stage of unmanaged exposure.

5. EMBEDDED ACCESS, NOT PERIMETER BREACH, DEFINES STRATEGIC RISK

The traditional perimeter of the enterprise has dissolved. Attackers are targeting identity systems, cloud control planes, collaboration platforms, and network-edge infrastructure. These environments blur the line between legitimate and malicious activity, complicating detection and containment.

State-aligned actors are pre-positioning within telecommunications, cloud environments, and infrastructure for long-term persistence. Criminal actors are monetizing the same surfaces. Examples observed in 2025 include Operational Relay Box networks built from compromised SOHO routers, collaboration platform abuse for command-and-control, GraphQL API exploitation, and dedicated malware such as FrostyGoop targeting industrial control systems.

AI as both acceleration layer and attack surface

AI amplified existing attacker playbooks rather than introducing entirely new categories, which ultimately compressed the time from initial access to impact. This was illustrated by threat actors using generative AI to scale phishing and reconnaissance, refine scripts, and accelerate ransomware operations.

At the same time, AI infrastructure became a target, indicating that familiar weaknesses are now appearing inside fast-moving AI ecosystems. Unsafe deserialization in model servers, token exposure in self-hosted platforms, orchestration framework injection risks, and supply chain compromises such as the malicious postmark-mcp package were all found within our data.

AI must therefore be governed as privileged infrastructure. Properly maintained inventories, access control, segmentation, and token monitoring are essential. At the same time, AI-augmented security operations are increasingly necessary to match adversary speed.

Industry and geographic targeting

North America accounted for 82% of observed incidents, with the United States representing roughly 70% of leak posts. Manufacturing, business services, and retail were the most frequently targeted industries, with healthcare and government also heavily impacted.

These sectors combine sensitive data, financial liquidity, and supply chain leverage, making them attractive for both extortion and strategic pre-positioning.

Strategic guidance for 2026

The data highlights a structural mismatch between attacker velocity and traditional defensive processes. Closing that gap requires a shift toward preemptive security as an operating model.

In 2026, we recommend that CISOs:

- Prioritize continuous visibility of assets and identities
- Enforce consistent multi-factor authentication
- Harden edge infrastructure
- Treat SaaS and AI as production-critical systems
- Augment detection and response workflows with automation and AI to speed up investigation timelines

Some exposure will be exploited; at this point, it's a natural part of the cycle. Therefore, resilience planning should take that into account. Immutable backups, tested recovery, credential resets, and rehearsed incident response processes are essential safeguards.

Final takeaway

The 2026 threat landscape is defined by acceleration. Exploitation is now faster, access is commoditized, and ransomware is industrialized.

However, the core vulnerabilities are not new. Weak credentials, exposed services, and unpatched edge systems remain consistently used vectors. What has changed is how quickly those weaknesses are identified, packaged, and weaponized.

For CISOs, competitive advantage now lies in clarity of exposure. The organizations that continuously understand their attack surface and reduce risk before exploitation will be best positioned to withstand the accelerated cyber attack cycle.

GET THE REPORT

ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our website, check out our blog, or follow us on LinkedIn or X.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**