NEWS RELEASE

Rapid7 2026 Global Threat Landscape Report Shows Exploited High and Critical-Severity Vulnerabilities Surged 105% as Attack Timelines Collapsed

2026-03-18

New research reveals exploitation now occurs within days of disclosure, reinforcing the need for preemptive security operations

BOSTON, March 18, 2026 (GLOBE NEWSWIRE) -- **Rapid7** (NASDAQ: RPD), a global leader in AI-powered managed cybersecurity operations, today released **The 2026 Global Threat Landscape Report: Decoding the Accelerated Cyber Attack Cycle**. The report finds that the window between vulnerability disclosure and confirmed exploitation continues to collapse, leaving organizations with dramatically less time to assess risk, prioritize remediation, and contain threats before impact. The predictive lead time defenders once relied on between disclosure and exploitation has largely disappeared.

The report found that exploited high and critical severity vulnerabilities more than doubled year over year, increasing 105% from 71 in 2024 to 146 in 2025, while the window between vulnerability publication and confirmed exploitation continues to shrink, with attackers increasingly operationalizing vulnerabilities within days of disclosure.

“Exploitation timelines are increasingly measured in days rather than weeks,” said Raj Samani, chief scientist at Rapid7. “AI is being integrated rapidly into attacker playbooks, accelerating how quickly exposure is operationalized. Many of the incidents we investigate still originate from known, unaddressed exposure. In those cases, attackers don’t need sophistication, they need opportunity. As remediation windows shrink, reducing that opportunity becomes essential to limiting compromise.”

Key findings from the 2026 report

This report correlates vulnerability publication data, confirmed exploitation trends, frontline MDR incident response telemetry, and dark web, cybercrime, and nation-state intelligence to provide a unified view of how exposure evolves into compromise.

Key findings include:

- Exploitation is accelerating faster than defenders can remediate: The number of “high-risk but not yet exploited” vulnerabilities (CVSS 7-10) fell dramatically, while the number of exploited vulnerabilities increased sharply from 71 in 2024 to 146 in 2025. This indicates that high-probability vulnerabilities (CVSS 7-10) are being operationalized almost immediately.
- Weaponization timelines continue to shrink: The median time from a vulnerability's publication to its inclusion in the CISA KEV catalog dropped from 8.5 days to 5.0 days, and the mean time dropped from 61.0 days to 28.5 days, a trend measured specifically among high- and critical-severity vulnerabilities.
- Identity exposure remains the dominant intrusion path: Valid accounts with missing or lax multi-factor authentication (MFA) accounted for 43.9% of all incident response investigations by Rapid7 in 2025, making it the single most common initial access vector.
- Ransomware is an industrialized monetization engine: Ransomware was involved in 42% of Rapid7 MDR incident response investigations last year. Additionally, total ransomware leak posts increased 46.4% year over year, rising to 8,835 in 2025.
- AI is accelerating attacker operations: Generative AI has evolved into a legitimate force multiplier, enabling adversaries to accelerate phishing content creation, scripting, and iterative problem solving.
- Advanced persistent threat (APT) campaigns adopt refined evasion techniques: Rapid7 has observed APT groups significantly evolving their techniques for staying off defenders’ radar. For example, Earth Kurma pioneered a “Living Off the App” strategy that covertly uses Cisco Webex for command-and-control, while Volt Typhoon now utilizes Living Off the Land techniques to maintain long-term persistence.

What this means for security operations

The report underscores that delayed remediation and misaligned prioritization are increasingly central to breach outcomes. As exploitation timelines compress, organizations must address exposure earlier and integrate more closely with detection and response. Attack surface exposure must now be triaged in the context of active attacker behavior, aligning remediation timelines with exploitation velocity to sustain durable cyber resilience.

"The challenge moving forward is less about identifying every vulnerability and more about understanding exposure, prioritizing realistically, and responding within increasingly compressed timelines," said Christiaan Beek, vice president of cyber intelligence at Rapid7. "Predictive lead time is a thing of the past. Now, it’s about your ability

to move smarter, not just faster. Organizations that reduce the preventable conditions attackers monetize before exploitation occurs, can regain a measure of control."

The 2026 report reinforces that operating preemptively is no longer optional. As adversaries embed AI into reconnaissance and exploitation workflows, defensive operations must evolve with the same discipline. Organizations that manage exposure, and integrate it into detection and response, will be better equipped to limit compromise and sustain durable cyber resilience.

To read a full copy of the report, visit **https://www.rapid7.com/research/report/global-threat-landscape-report-2026/**.

About the Rapid7 2026 Global Threat Landscape Report

The Rapid7 2026 Global Threat Landscape Report, Decoding the Accelerated Cyber Attack Cycle, is an in-depth global adversary behavior analysis from Rapid7 Labs. Drawing on telemetry from the company's managed detection and response (MDR) investigations, vulnerability intelligence, and frontline incident response, the report examines the collapse of the window between disclosure and exploitation, the industrialization of ransomware, and the role of AI as an acceleration layer in modern attack campaigns. This report provides a data-driven view of how exploitation speed, identity exposure, and strategic pre-positioning are reshaping enterprise cyber risk.

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 Media Relations
Stacey Holleran
Sr. Manager, Global Communications
press@rapid7.com
(857) 216-7804

Rapid7 Investor Contact
Matt Wells

Vice President, Investor Relations
investors@rapid7.com
(617) 865-4277

Source: Rapid7