NEWS RELEASE

Rapid7 Q1 2026 Threat Landscape Report Finds Vulnerability Exploitation Overtakes Social Engineering as the Top Initial Access Vector

2026-05-21

New research highlights how AI-driven exploitation, zero-click vulnerabilities, and fragmented ransomware operations are reshaping cyber risk

BOSTON, May 21, 2026 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a global leader in AI-powered managed cybersecurity operations, released its Q1 2026 Threat Landscape Report, **examining** trends in vulnerability exploitation, ransomware activity, and cybercriminal infrastructure. The report found that vulnerability exploitation surpassed social engineering as the leading initial access vector, accounting for 38% of incident response cases. The shift reflects the growing role of AI in accelerating how quickly attackers can identify, weaponize, and exploit unpatched systems at scale, compressing the window defenders have to respond.

Reinforcing this trend, half of vulnerabilities actively exploited in the wild during Q1 were zero-click, network-facing issues requiring no authentication or user interaction, giving attackers direct access to exposed systems without relying on human action. The finding reinforces trends identified in **Rapid7's 2026 Annual Global Threat Landscape Report**, which found that exploitation timelines continue to shrink: among high- and critical-severity vulnerabilities, the median time from public disclosure to inclusion in CISA's Known Exploited Vulnerabilities (KEV) catalog fell from 8.5 days to 5.0 days.

"We've spent years building a security culture around humans being the weakest link, but our Q1 findings show AI is quietly rewriting that equation," said Raj Samani, SVP and Chief Scientist at Rapid7. "Attackers are increasingly bypassing user interaction altogether, prioritizing direct access to exposed infrastructure and dramatically narrowing the window defenders have to respond."

Drawing on select tracked CVEs, MDR incident response data, ransomware leak-site intelligence, and dark web telemetry, the report highlights evolving exploitation patterns, ransomware activity, and changes in attacker infrastructure.

Key findings include:

- Vulnerability exploitation was the leading initial access vector in MDR data: Exploitation accounted for 38% of incident response cases, followed by social engineering (24%) and compromised accounts (14%).
- Zero-click, network-facing vulnerabilities dominated exploited CVEs: Half of vulnerabilities actively exploited in the wild during Q1 required no authentication or user interaction, enabling direct access to exposed systems.
- Public discussion preceded exploitation activity: Exploited vulnerabilities averaged 1.8 million mentions across blogs, forums, and social media, indicating that widely discussed vulnerabilities can quickly become operational targets.
- SQL injection became the most exploited vulnerability type: SQL injection overtook OS command injection in Q1, reflecting attacker focus on common, broadly distributed web application weaknesses.
- Ransomware activity remained fragmented across groups: Qilin led leak-site activity with 357 posts, followed by The Gentlemen (206) and Akira (174), indicating ransomware activity remained fragmented across operators.
- Abused Remote Monitoring and Management (RMM) tools were the most prevalent threat category: RMM tools accounted for 22.9% of observed activity, followed by ClickFix (18.8%) and Windows Native Scripts (10.4%).

What this means for security operations

As exploitation timelines continue to shrink, security teams face increasing pressure to identify, prioritize, and remediate exposed systems before attackers can operationalize vulnerabilities at scale.

“Q1 shows how quickly exposed systems can become operational targets,” said Christiaan Beek, Vice President of Cyber Intelligence at Rapid7. “Security teams can’t apply the same level of investigation and response across every signal when attackers are consistently prioritizing what they can reach and exploit. That gap is where risk accumulates.”

To read a full copy of the report, visit **https://www.rapid7.com/research/report/threat-landscape-report-2026-q1/**.

About the Rapid7 Q1 2026 Threat Landscape Report

The Rapid7 Threat Landscape Report is a quarterly analysis of global adversary behavior drawn from the company's managed detection and response operations, vulnerability intelligence platforms, and threat research telemetry. The Q1 2026 edition examines the impact of vulnerability exploitation, geopolitical cyber activity, ransomware evolution, and cybercriminal infrastructure.

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
Alice Randall
Director, 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