NEWS RELEASE

Rapid7 Report: Human Operators Still Drive Most of Tracked Cyberattacks, but Exploitation Windows Are Narrow

2026-10-21

Attacker adoption of agentic AI is lagging the technology, but adversaries are already exploiting high-severity vulnerabilities in an average of just three days, leaving defenders a narrow window to reduce exposure

BOSTON, Oct. 21, 2026 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leader in AI-powered managed cybersecurity operations, today released its **Quarterly Threat Landscape Report**, revealing that human operators remain the primary drivers of modern cyber threats despite widespread warnings about autonomous AI attacks.

The report shows AI is used as an operational component in just 8% of tracked incidents. While automation increasingly handles tactical execution, human actors still select most targets and dictate attack intent. Drawing from vulnerability research, frontline incident response, and underground monitoring, the newly announced **Rapid7 Intelligence** connects these insights to deliver a comprehensive view of adversary operations.

"Board decks often confuse the real explosion in AI-driven vulnerability discovery with actual exploitation, which hasn't materialized. Only 8% of tracked reporting cites AI as an operational component," said Christiaan Beek, Vice President of Rapid7 Intelligence. "But that's a snapshot of adoption, not a ceiling. Agentic capabilities are advancing faster than any organization, attackers included, can rework its processes around them. The question is when, not if, agentic exploitation scales. Defenders need to move past reactive patching and start grounding their risk appetite in concrete days of exposure."

Key findings include:

- Vulnerability exploitation continues to accelerate: Attackers exploit high-severity vulnerabilities within an

average of just three days, with 71% occurring in the first week—underscoring the urgent need to address critical exposures faster than traditional patching cycles allow.

- U.S. organizations accounted for the largest volume of ransomware listings. Rapid7 recorded 1,112 U.S. ransomware leak-site listings, roughly eight times Germany's total, with The Gentlemen (342), Qilin (339), and INC Ransom (99) leading group activity.
- "Holy Grail" vulnerabilities drive attacks. 79% of exploited flaws required no authentication and no user interaction, giving adversaries direct, remote access into enterprise environments.
- Compromised access drove underground market activity. Of 63 monitored posts, 41 advertised Remote Desktop Protocol (RDP) or network access.

Across espionage and cybercrime campaigns, threat groups change, but core tactics persist, including command and scripting interpreters, credential theft, and remote-access exploitation. These patterns underscore the need for behavioral detection and response, not static lists of known groups.

What this means for security operations

The findings from the third quarter of 2026 point to clear priorities for security teams: identify exposed assets, assess what attackers can exploit, and prioritize fixes by business impact. While the report findings show cyber threats remain human-driven, attackers are still leveraging AI to accelerate campaigns, making it critical for defenders to rapidly patch remotely exploitable vulnerabilities rather than wait for scheduled updates.

To read a full copy of the report, visit **here**.

About the Rapid7 Quarterly 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 Q3 2026 edition examines vulnerability exploitation, state-aligned and cybercrime activity, ransomware trends, and underground markets.

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.

Media Contact
Christine Nurnberger
SVP Global Marketing and Growth
press@rapid7.com

Rapid7 Investor Contact
Christopher Keenan
Vice President, Deputy General Counsel
investors@rapid7.com

Source: Rapid7