NEWS RELEASE

Rapid7 Q3 Threat Report Reveals Ransomware Alliances, AI Weaponization, and the Obsolescence of “Time to Patch”

2025-11-12

BOSTON, Nov. 12, 2025 (GLOBE NEWSWIRE) -- **Rapid7**, a leader in threat detection and exposure management, today released its **Q3 2025 Threat Landscape Report**, revealing how threat actors are accelerating the race between vulnerability disclosure and exploitation, consolidating ransomware power structures, and increasingly weaponizing artificial intelligence to evade detection. The report draws from Rapid7’s Intelligence Hub, AttackerKB, incident response, and managed detection and response (MDR) telemetry, offering data-driven insight into how adversaries are evolving and how defenders can adapt.

“Ransomware has evolved significantly beyond its early days to become a calculated strategy that destabilizes industries,” said Raj Samani, Chief Scientist at Rapid7. “In addition, the groups themselves are operating like shadow corporations. They merge infrastructure, tactics, and PR strategies to project dominance and erode trust faster than ever.”

Critical vulnerability exploitation speeds up as old weaknesses persist

Rapid7’s quarterly analysis shows that the total number of newly exploited vulnerabilities trended downward, dropping 21% from Q2 to Q3. However, adversaries doubled down on older, unpatched weaknesses, including CVEs more than a decade old, indicating that historic exposures remain potent attack vectors.

The mass exploitation of critical vulnerabilities in Microsoft SharePoint (CVE-2025-53770) and Cisco ASA/FTD products underscores the narrowing window between patch disclosure and in-the-wild attacks.

“The moment a vulnerability is disclosed, it becomes a bullet in the attacker’s arsenal,” said Christiaan Beek, senior director of threat intelligence and analytics at Rapid7. “Attackers are no longer waiting. Instead, they’re weaponizing vulnerabilities in real time and turning every disclosure into an opportunity for exploitation. Organizations must now assume that exploitation begins the moment a vulnerability is made public and act accordingly.”

Ransomware activity spikes with new alliances and innovative tactics

The quarter also saw 88 active ransomware groups, up from 65 in Q2 and 76 in Q1, signaling an increase in activity as well as underscoring these groups’ fluidity. Groups like Qilin, SafePay, and WorldLeaks led a wave of alliances targeting industries like business services, manufacturing, and healthcare, and experimenting with fileless operations, single-extortion data leaks, and affiliate service offerings such as ransom negotiation assistance, where a more senior member of the group partners with a less experienced player to extort the victim.

Generative AI lowers barriers as nation-state campaigns redefine cyber warfare

The report details how generative AI is lowering the barrier for creating convincing phishing campaigns and enabling adaptive malware, such as LAMEHUG, which can dynamically generate new commands.

Meanwhile, nation-state operators from Russia, China, and Iran refine their tactics, blurring the line between espionage and disruption by targeting supply chains and identity systems with an emphasis on stealth and persistence.

To read a full copy of the report, visit **https://www.rapid7.com/research/report/threat-landscape-report-2025-q3/**.

About the Rapid7 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 2025 edition provides one of the most comprehensive views of the global threat ecosystem: from ransomware and zero days to state-sponsored operations and AI-driven attacks.

About Rapid7

Rapid7, Inc. (NASDAQ: RPD) is on a mission to create a safer digital world by making cybersecurity simpler and more accessible. We empower security professionals to manage a modern attack surface through our best-in-class technology, leading-edge research, and broad, strategic expertise. Rapid7’s comprehensive security solutions help more than 11,000 global customers unite cloud risk management with threat detection and response to reduce

attack surfaces and eliminate threats with speed and precision. 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
Ryan Gardella / Ryan Flanagan
ICR, Inc
investors@rapid7.com
(617) 865-4277

Source: Rapid7