NEWS RELEASE

Rapid7 Access Brokers Report: New Research Reveals Depth of Compromise in Access Broker Deals, with 71% Offering Privileged Access

2025-08-12

Initial access brokers are selling more than just a way in; Rapid7 calls for unified detection, intelligence, and automation to disrupt these cyberattacks early

BOSTON, Aug. 12, 2025 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leader in threat detection and exposure management, today released its **2025 Access Brokers Report**, a new research analysis of illicit underground marketplaces where cybercriminals buy and sell access to corporate networks. Drawing on six months of threat intelligence from dark web forums Exploit, XSS, and BreachForums, the report uncovers new insights into how initial access to compromised businesses is being sold — often for less than $1,000 — and the steps defenders can take to disrupt the process in its earliest stages.

Rapid7's threat intelligence researchers analyzed hundreds of posts by Initial Access Brokers (IABs) offering access to compromised networks across a range of industries and regions. Their findings paint a stark picture: "initial" access doesn't necessarily equate to minimal; in many cases, this access represents a deep compromise.

"This report shows that initial access brokers aren't intent upon finding a single way into an organization's network and then quickly exiting — they're making attempts to explore the networks they've infiltrated. And they're often succeeding," said Raj Samani, SVP and chief scientist at Rapid7. "In doing so, the IAB can offer buyers admin privileges, multiple access types, or both. By the time a threat actor logs in using the access and privileged credentials bought from a broker, a lot of the heavy lifting has already been done for them. Therefore, it's not about if you're exposed, but whether you can respond before the intrusion escalates."

Key report findings include:

- The vast majority of access broker sales (71.4%) offer more than just a specific access vector; they also include a level of privilege — and in nearly 10% of those sales, it's a bundle with multiple initial access vectors and/or privileges.
- The average sale price hovered just over $2,700, with nearly 40% of offerings priced between $500–$1,000.
- VPN, Domain User, and RDP were the most common access types — the very same weak points seen in Rapid7's **incident response investigations**.

The Access Brokers Report arrives as security teams grapple with alert fatigue, limited resources, and evolving attacker tradecraft. It supports Rapid7's growing body of evidence that exposure management and threat detection must be operationalized together, not handled in isolation.

This vision underpins the company's recent launch of **Incident Command**, an AI-native SIEM that unifies prevention, detection, intelligence, and response within a single workflow. With its seamless integration of **Intelligence Hub**, Incident Command gives security teams direct access to the same curated threat insights that informed this report — now embedded into detection logic and investigation workflows.

In addition to in-depth forum analysis, the report outlines concrete steps organizations can take to harden defenses and reduce attacker dwell time:

- Enforce MFA — especially on VPN, RDP, and user accounts that access critical infrastructure.
- Invest in threat-informed detection and response — including unified platforms that correlate access signals with suspicious activity.
- Run regular red team exercises to identify exposure paths like abandoned accounts, default credentials, and externally accessible RDP services.

This research reinforces Rapid7's position that threat detection and exposure management must be fast, unified, and context-rich. As highlighted in the company's recognition in the 2025 **Frost Radar for MDR**, operationalizing threat intelligence, asset context, and automation isn't just a best practice — it's a requirement.

Initial Access Brokers and the forums they use have long been analyzed by threat intelligence teams. While law enforcement activity and takedowns continue, access brokers remain a persistent threat to organizations around the world.

To read a full copy of the report, visit **https://www.rapid7.com/lp/initial-access-brokers-report/**.

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
Stacey Holleran
Sr. Manager, 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