NEWS RELEASE

Rapid7 Ransomware Radar Report Charts Ransomware Group Activity and Methodologies for Fresh Insights

8/6/2024

New Rapid7 research analyzes more than 70 active ransomware groups, 21 of which were new in 2024

LAS VEGAS, Aug. 06, 2024 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leader in extended risk and threat detection, today announced the release of its **Ransomware Radar Report** in conjunction with the company's presence at **Black Hat USA**. The all-new research report provides a fresh perspective on the global ransomware threat by analyzing, comparing, and contrasting attacker activity and techniques over an 18-month period ending June 30, 2024.

According to the report, ransomware groups continue to refine their craft, building and scaling business models that resemble legitimate corporate enterprises. They market their services to prospective buyers, offer company insiders commissions in exchange for access, and run formal bug bounty programs. In addition, Rapid7 researchers found three major clusters of ransomware families with similar source code, indicating that ransomware groups are focusing their development efforts on quality over quantity.

"The Ransomware Radar Report uses data to tell the story of how ransomware and the threat actors that wield it are evolving," said Christiaan Beek, senior director, threat analytics at Rapid7. "For example, the related source code, combined with a continuing decline in the number of unique ransomware families, suggests a move toward more specialized and highly effective ransomware variants, rather than a broad array of less sophisticated malware."

Additional key findings from the Ransomware Radar Report include:

- 21 new groups have surfaced: Within the first six months of 2024, Rapid7 observed 21 new ransomware groups entering the scene. Some of these groups are brand new while others are previously known groups rebranding under a new name. One of the most notable of these new groups, RansomHub, has quickly established itself as a prominent extortion group by making 181 posts to its leak site between February 10 and June 30, 2024.
- Leak site posts are up 23%: Each leak site post represents an extortion attempt. The number of ransomware groups actively posting to leak sites is increasing, from an average of 24 groups posting per month in the first half (H1) of 2023 to 40 per month in H1 2024. Furthermore, 68 ransomware groups made a total of 2,611 leak site posts between January and June, representing a 23% increase in the number of posts made in H1 2023.
- Smaller organizations have become a more frequent target: In examining the revenue distribution of companies listed within access broker postings, Rapid7 noted that companies with annual revenues around $5 million are falling victim to ransomware twice as often as those in the $30-50 million range and five times more frequently than those with a $100 million revenue. This finding could suggest that such companies are large enough to hold valuable data but not as well protected as their larger counterparts.

“The report’s insights into the ransomware landscape are crucial for informing Defenders’ cybersecurity strategies,” said Beek. “From our own detection engineering point of view, the clusters and additional report information, such as the usage and type of encryption algorithms, help us uplevel hunting techniques and prevention, detection, and response technologies. Rapid7 continually investigates new techniques used by threat actors and ransomware operators, tests them against our patented Ransomware Prevention technology, and creates new preventions to ensure customers are protected against the latest threats.”

Security practitioners and other stakeholders fighting ransomware can access the full report now at **https://www.rapid7.com/research/report/ransomware-radar-report/**. The schedule of Rapid7’s Black Hat USA events and on-site meeting request form are both available here: **https://rapid7.registration.goldcast.io/events/015dcea6-f4ab-4258-8004-58dfdec9c959**.

About the Ransomware Radar Report

The Rapid7 Ransomware Radar Report provides a comprehensive analysis of ransomware incidents and binaries recorded and gathered globally, offering insights into trends, attacker profiles, ransomware families, and the implications for cybersecurity defenses. The data used for the report comes from Rapid7’s incident response teams and independent Rapid7 Labs research. The ransomware sample dataset used consists of (i) prevalent and available ransomware families from 2023 which continued their operations into 2024, and (ii) new 2024 ransomware samples that were observed until the end of June, 2024.

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
Elizabeth Chwalk
Sr. Director, Investor Relations
investors@rapid7.com
(617) 865-4277

Source: Rapid7