NEWS RELEASE

Rapid7 Releases Attack Intelligence Report Examining High-Impact Attacks and Vulnerability Data Trends

5/21/2024

Multi-year trend shows more zero-day vulnerabilities leading to mass compromise events

BOSTON, May 21, 2024 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leader in extended risk and threat detection, today announced the release of its **2024 Attack Intelligence Report**. The report provides expert insights and guidance that security practitioners can use to better understand and anticipate modern cyber threats.

The research underpinning the Attack Intelligence Report is based on more than 1,500 curated vulnerability and exploit data points; analysis of 180-plus advanced threat campaigns; thousands of tracked ransomware incidents, extortion communications, and dark web posts; and insights from trillions of security events across Rapid7 MDR and threat analytics telemetry.

Several significant findings arose from this vast examination of information dating back to 2019 and as recent as early 2024. For example, in 2023, for the second time in the last three years, more mass compromise events arose from zero-day vulnerabilities (53%) than from n-day vulnerabilities. Last year's numbers represent a return to 2021 levels of widespread zero-day exploitation (52%), following a slight respite (43%) in 2022.

"Our data shows 2021 to have been the dividing line between a 'then' and a 'now' in zero-day attacks," said Caitlin Condon, director of vulnerability intelligence at Rapid7 and the report's primary author. "Since that time, the median number of days between vulnerability disclosure and exploitation, which we began tracking several years ago, has stayed in single digits across the CVEs in our annual datasets; widespread exploitation of major vulnerabilities has shifted from a notable event to a baseline expectation; and ransomware attacks regularly take entire public-facing systems offline, sometimes for weeks or months at a time."

In addition to a consistently high number of zero days leading to mass compromise events, the report notes a "pronounced shift" in the way these events are playing out. Instead of following the historical pattern of "many attackers, many targets," nearly a quarter (23%) of widespread threat CVEs Rapid7 examined in 2023 and early 2024 arose from well-planned, highly orchestrated zero-day attacks in which a single adversary compromised dozens or even hundreds of organizations at once, often leveraging custom tooling like proprietary exploits and backdoors.

Additional key findings from the 2024 Attack Intelligence Report include:

- Mass compromise events stemming from exploitation of network edge devices have almost doubled since the start of 2023, with 36% of widely exploited vulnerabilities occurring in network perimeter technologies. More than 60% of the vulnerabilities Rapid7 analyzed in network and security appliances in 2023 were exploited as zero-days.
- While skilled adversaries are still fond of memory corruption exploits, most of the widely exploited CVEs from the past few years have arisen from simpler, more easily exploitable root causes, like command injection and improper authentication issues.
- 41% of incidents Rapid7 MDR observed in 2023 were the result of missing or unenforced multi-factor authentication (MFA) on internet-facing systems, particularly VPNs and virtual desktop infrastructure.
- Rapid7 Labs tracked more than 5,600 separate ransomware incidents over the course of 2023 and the first few months of 2024. The number of unique ransomware families reported across 2023 incidents decreased by more than half, from 95 new families in 2022 to 43 in 2023.

"This is a mature, well-organized cybercrime ecosystem at work, with increasingly sophisticated mechanisms to gain access, establish persistence, and evade detection," said Condon. "The data is telling us that we are experiencing the intensification of a multi-year trend; now more than ever, implementing zero-day patching procedures for critical technologies is key."

The report notes that network edge devices are at particular risk of n-day and zero-day exploitation, and Rapid7 recommends that vulnerabilities in these devices be mitigated as soon as vendor-provided patches or workarounds are available. The report also indicates that enabling logging and ensuring it is working as expected are critical for allowing security operations teams to hunt for the more elusive indicators of compromise and suspicious activity representing incidents executed by the mature attacker groups identified in the research.

To access the complete Rapid7 2024 Attack Intelligence Report, which includes additional practical guidance for defenders, visit **https://www.rapid7.com/research/report/2024-attack-intelligence-report/**.

About the 2024 Attack Intelligence Report

Since 2020, Rapid7 has released an annual Vulnerability Intelligence Report with curated vulnerability data and in-depth analyses of exploit trends. In an effort to broaden the scope of this research and offer a more holistic view of the attack landscape, this year's report — renamed The Attack Intelligence Report — combines vulnerability and exploit research with hands-on data from Rapid7's managed detection and response (MDR) division, as well as the company's threat analytics and emergent threat response teams.

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. Product & Research Communications Manager
press@rapid7.com
(857) 216-7804

Rapid7 Investor Contact
Elizabeth Chwalk
Sr. Director, Investor Relations
investors@rapid7.com
(617) 865-4277

Source: Rapid7