RAPID7

SPEED IS NO LONGER THE ADVANTAGE

Security did not fall short last year because teams were slow. Automation, artificial intelligence, and industrialized access markets have compressed the time between exposure and impact. What once took weeks now takes days. In some cases, minutes.

In other words: The predictive window has collapsed.

High-risk vulnerabilities are exploited almost immediately. Valid credentials are packaged and sold. Ransomware operators move from access to data theft in hours.

And the data prove it.

EXPLOITATION IS ACCELERATING

105% INCREASE

Confirmed exploitation of newly disclosed CVSS 7–10 vulnerabilities **71 in 2024 → 146 in 2025**

20X GROWTH IN FOUR YEARS

7 exploited vulnerabilities in 2022 **→ 146 in 2025**

EXPLOITATION RATE UP 8X

<0.1% of disclosures in 2022 **→ 0.8% in 2025**

TIME TO EXPLOITATION IS SHRINKING

MEDIAN TIME TO CISA KEV INCLUSION 8.5 → 5 DAYS
MEAN TIME 61 → 28.5 DAYS

High-risk but not yet exploited vulnerabilities are disappearing.

338 HIGH-RISK UNEXPLOITED VULNS IN 2024 → 65 IN 2025

The window between exposure and impact is closing.

MOST ATTACKS START WITH KNOWN EXPOSURE

43.9% Valid accounts without multi-factor authentication

24.6% Vulnerability exploitation

7% Exposed services

Initial access is preventable. It is also predictable.

INITIAL ACCESS IS NOW INDUSTRIALIZED

Underground marketplace listings in 6 months:

221 ON DARKFORUMS
208 ON RAMP

Most common access types: 21.2% RDP, 12.8% VPN, 11.2% RDWeb

Exposure is packaged and sold at scale.

RANSOMWARE IS BIG BUSINESS

42% OF RAPID7 MDR INVESTIGATIONS INVOLVED RANSOMWARE

46.4% INCREASE IN LEAK POSTS YEAR OVER YEAR 6,034 → 8,835

102 → 140 ACTIVE RANSOMWARE GROUPS

ATTACKERS ARE USING AI TO SCALE

AI is not introducing entirely new categories of attacks. It is accelerating existing playbooks.

GENERATIVE AI IS USED TO: SCALE PHISHING AND RECONNAISSANCE, REFINE SCRIPTS AND ACCELERATE RANSOMWARE OPERATIONS

The result: faster initial access, faster lateral movement, faster impact.

HOW TO BUILD RESILIENCE

Shift from reacting to incidents to reducing exposure before it is exploited. Maintain continuous visibility into assets and identities, enforce multi-factor authentication, harden edge and SaaS systems, use automation to accelerate response, and plan for resilience when exploitation occurs.

GET THE REPORT TO HELP YOU STAY AHEAD →

RAPID7