RAPID7

rapid7.com

2024 Attack Intelligence Report:

Insights From Four Years Of Vulnerability And Exploit Data

In the 2024 Attack Intelligence Report, Rapid7 examines four years' worth of vulnerability data and attacker behavior to help security practitioners understand the risks, motives, and threat actor tactics that permeate today's cyberthreat landscape. Below are some key insights.

A High Incidence Of Zero-Day Exploitation Has Become The Norm

The median time to known exploitation for CVEs Rapid7 has analyzed from 2020 onward

One Day

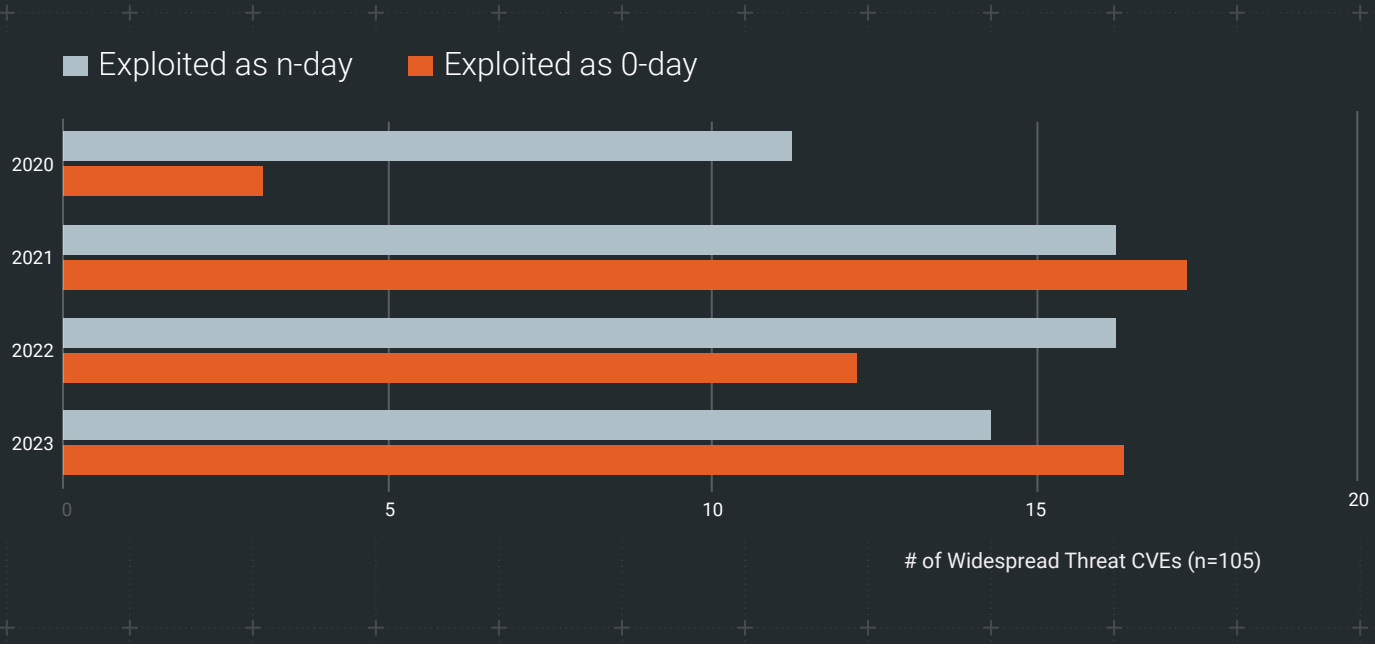
53% of CVE-based mass compromise incidents Rapid7 tracked between January 2023 and February 2024 arose from zero-day exploit

Network edge device exploits exploded — even more than in years past.

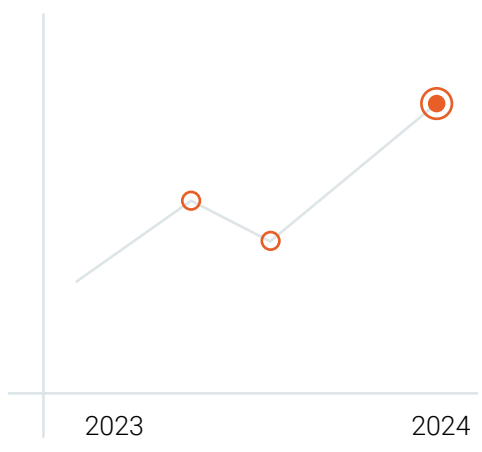
of 2023 widespread threats affected **network perimeter tech**

of vulns Rapid7 analyzed in network and security appliances **exploited as zero-days**

Widespread Threat CVEs 2020-2024



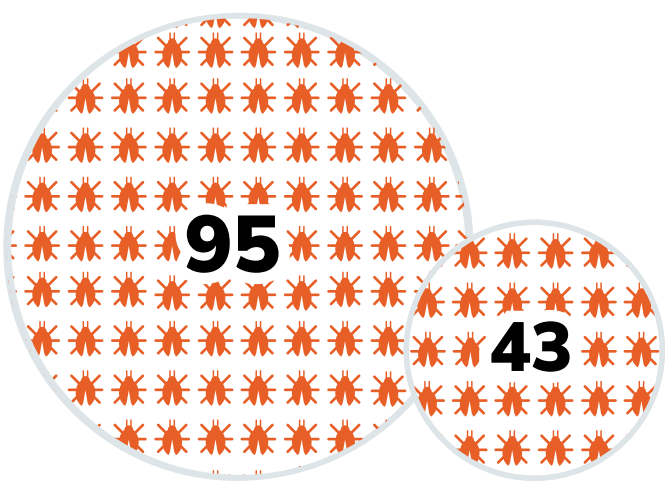
Ransomware Operations Are Fast, Furious, And More Devastating Than Ever



Rapid7 Labs tracked
5,600+ ransomware incidents between January 2023 and February 2024*

*This number doesn't reflect incidents that go unreported

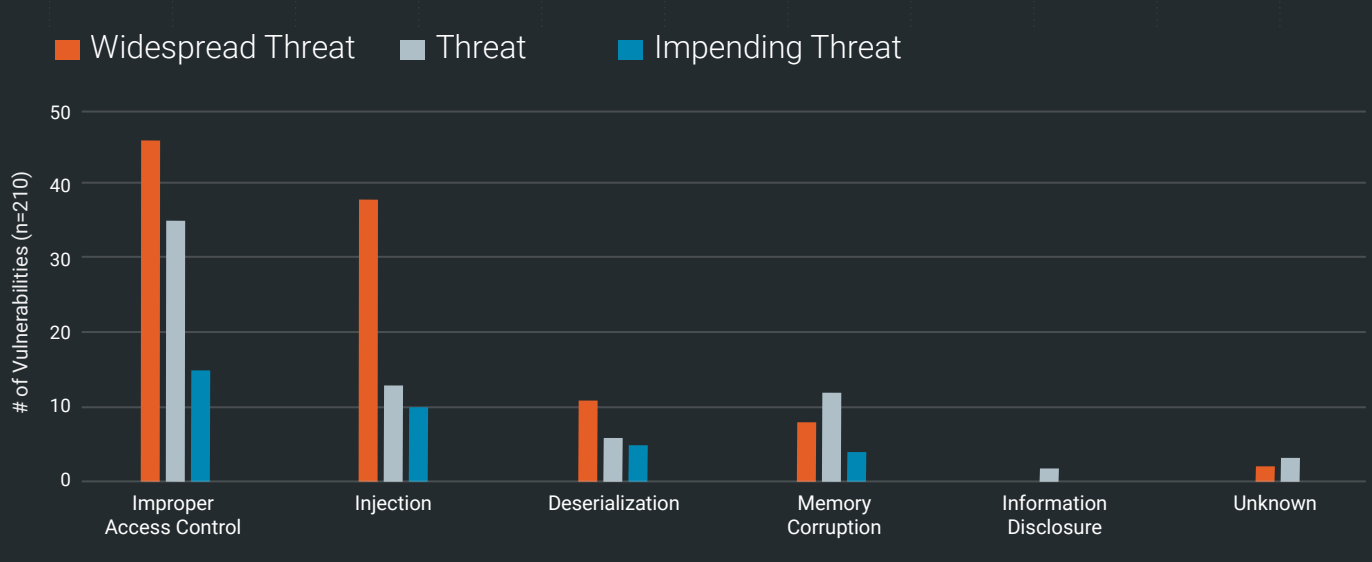
The # of new ransomware families is down by more than half
indicating that pre-existing models and capabilities remain profitable for attackers.



Root Cause Analysis Shows Adversaries Favor Exploits For Simple Vuln Classes

75% of notable CVEs Rapid7 analyzed since 2020 have improper access control and injection issues as their root causes

Vulnerability Classes and Threat Status 2020-2024



So What Do We Do?

How do we increase our resilience and readiness for today's cyberthreats? Some guidance:

40%

of incidents were due to missing or inconsistent MFA. Make MFA a top priority

Apply principles of least privilege: allow listing the standard; implement granular access control; regularly review and remove users

Implement a strong proactive vulnerability risk management program across cloud and on-prem

Create zero-day patching procedures for mission critical technology, particularly network edge devices

Doubling down on an offsite backup strategy helps organizations be more resilient to potential ransomware attacks

Download the full report at www.rapid7.com