RAPID7

QUARTERLY THREAT LANDSCAPE REPORT

The compression era: Q2 2026 has showed that traditional patch cycles are overwhelmed.

From Rapid7 Labs

RESEARCH REPORT

INTRODUCTION

Q2 2026 was not just another busy quarter in cyber. It felt more like a stress test of the way we currently manage exposure. Traditional patch cycles are being overwhelmed by the sheer volume of vulnerabilities and attacker speed and precision.

Vulnerabilities are being disclosed at higher volume, proof-of-concept code is appearing faster, exploitability is being tested earlier, and attackers are getting better at turning public information into operational access. For defenders, the issue is not simply that there is more to patch. The real issue is that the time between knowing about a weakness and seeing it used in the wild continues to collapse.

That changes the conversation.

This is no longer a world where security teams can rely on traditional patch rhythms, static severity scores, or quarterly prioritization exercises. Attackers have never waited for organizations to get their defenses ready before seeking out exposed systems. But now, they have greater means than ever to get out in front of outdated security programs.

The conversation around Anthropic's AI-assisted vulnerability discovery model, Mythos, and the broader "vulnpocalypse" narrative in cybersecurity circles belongs in this report, but not as science fiction and not as marketing fear. AI does not magically turn every vulnerability candidate into a working exploit nor is finding a bug the same as understanding exploitability.

Real-world exploitation still depends on context: reachable code paths, configuration, authentication state, target architecture and, for example, environmental constraints. For CISOs and security leaders the question is not whether every AI-assisted vulnerability lead becomes a real exploit. Most will not. The question is how much reachable, exploitable exposure an organization is willing to carry when capable adversaries can use automation, tooling, and expertise to move fast through discovery, validation, and targeting.

This is why preemptive security matters. Not as a slogan, but as an operating model.

Organizations cannot patch their way out of this by treating every vulnerability as equal. They need to understand what they expose, which assets matter, which weaknesses are actually reachable, which identities can be abused, and where detection must fire before initial access becomes lateral movement.

As you will see in this report, the lessons from Q2 are simple. To defend against an attacker that can compress time, defenders need to compress exposure.

Rapid7 Labs

KEY REPORT TAKEAWAYS

KEY TAKEAWAY 1

High-Severity Vulnerability Disclosures Double Year-Over-Year

Disclosures of high- and critical-severity vulnerabilities (CVSS 7-10) doubled year-over-year from 4,268 in Q2 2025 to 8,539 in Q2 2026. New exploited vulnerabilities increased 8% to 40 in Q2. Taken together this points to a widening gap between what's disclosed and what any team can realistically triage.

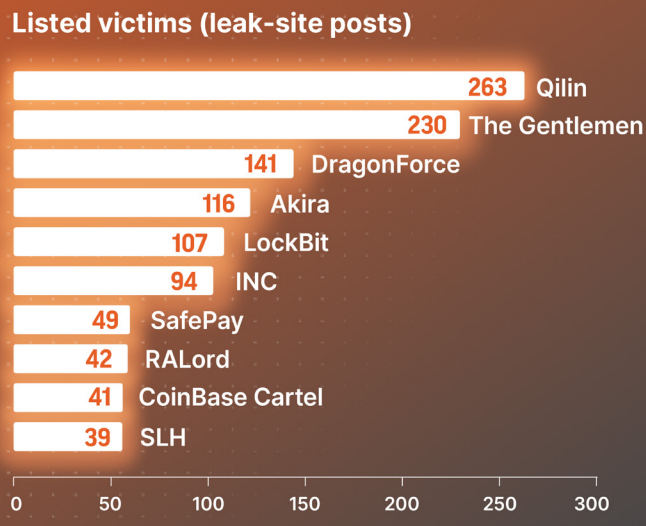
KEY TAKEAWAY 2

Rise in Zero-Interaction "Holy Grail" Vulnerabilities

The proportion of exploited vulnerabilities classified as "holy grail" (network-exploitable, no authentication, no user interaction) increased to 62% (25 of 40), a 9-point year-over-year jump compared to the 53% (24 of 45) observed in Q2 2025.

FIVE GROUPS DRIVE MOST OF THE RANSOMEWARE MARKET

Q2 2026 leak-site victim counts, top 10 groups



KEY TAKEAWAY 3

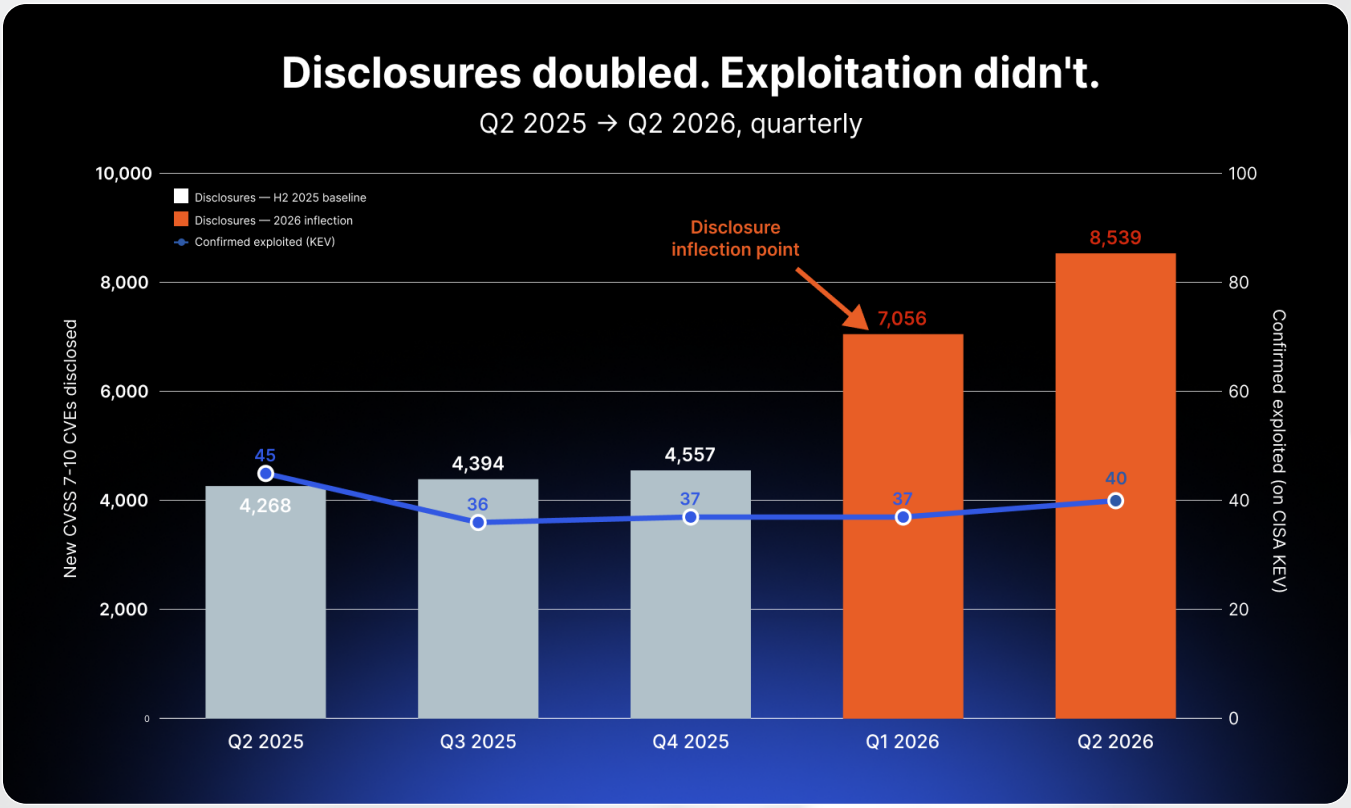
Persistent Targeting by Nation-State APT Clusters

State-aligned advanced persistent threat (APT) groups tied to Iran, North Korea and Russia ran sustained campaigns against finance, government, energy, manufacturing and healthcare.

KEY TAKEAWAY 4

A Busy Quarter for Dark Web Activity and Initial Access Trading

Dark web monitoring identified 124 exploit and access listings across 20 underground sources. Among the 23 CVEs being traded, most had proof-of-concept (PoC) code, and nearly 40% were exploited in the wild.



KEY TAKEAWAY 5

Ransomware Trends and High-Risk Sectors

Qilin led activity with 263 victims, while the United States accounted for 881 of all listed incidents, with business services and healthcare identified as the top targeted sectors.

GEOPOLITICAL ESCALATION

Q2 2026 featured multiple active nation-state groups targeting a wide variety of regions and industries.

Russian campaigns:

APT28 exploited SOHO edge routers for DNS hijacking, potentially allowing for the theft of authentication tokens and passwords.

Iranian campaigns:

A sustained industrial control systems/operational technology (ICS/OT) campaign targeting U.S. Programmable Logic Controllers (PLCs) — specifically Rockwell Automation and Allen-Bradley systems.

Top adversary techniques (MITRE ATT&CK)

- Application Layer Protocol: Web Protocols, T1071.001, Observed Count 90
- Obfuscated Files or Information, T1027, Observed Count 86
- Ingress Tool Transfer, T1105, Observed Count 70

THE VULNERABILITY INTELLIGENCE AND EXPLOIT LANDSCAPE

Critical exploit tracking

Q2 2026 is all about rapid attack, and rapid response.

Volume, speed:

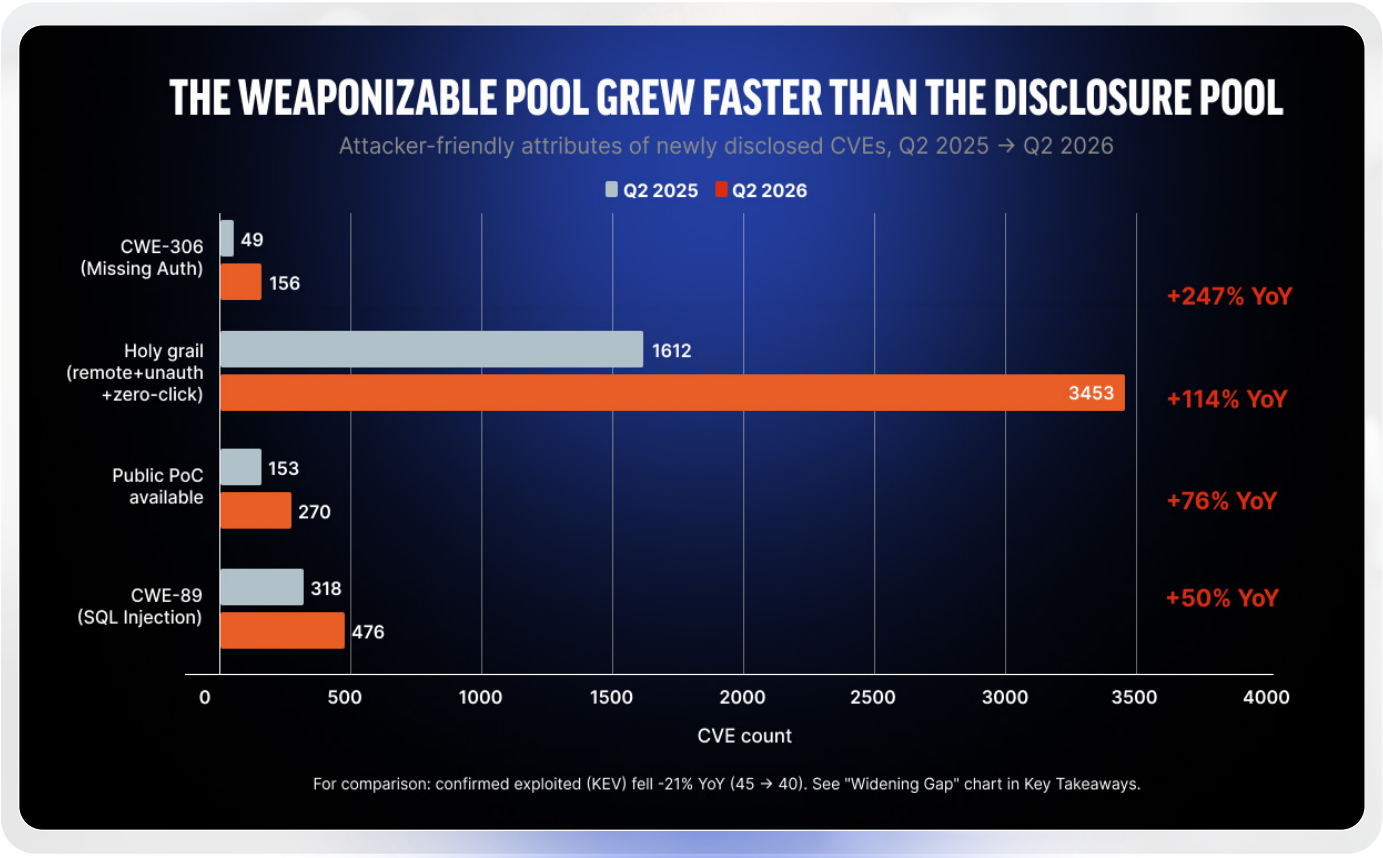
The volume of critical vulnerabilities, up 21% from last quarter, and the rate of publicly available proof-of-concept (PoC) code, are rising, up 12% from last quarter and 76% when compared to 2025 Q2. This indicates a growing number of easily weaponized threats.

Vulnerability disclosures doubled YoY:

8,539 new CVSS 7-10 CVEs in Q2 2026 vs 4,268 in Q2 2025 (+100%). Defenders need exposure context prioritization to keep pace, because attackers are already using AI to discover faster.

Attackers have a growing backlog of unauthenticated internet-facing endpoints to weaponize.

CWE-306 (Missing Auth) disclosures surged +247% YoY (156 vs 45); SQL Injection (CWE-89) +50% YoY (476 vs 318). Inventory your external attack surface and enforce authentication on every exposed endpoint before the exploitation curve catches up.



THREAT ACTOR ACTIVITY

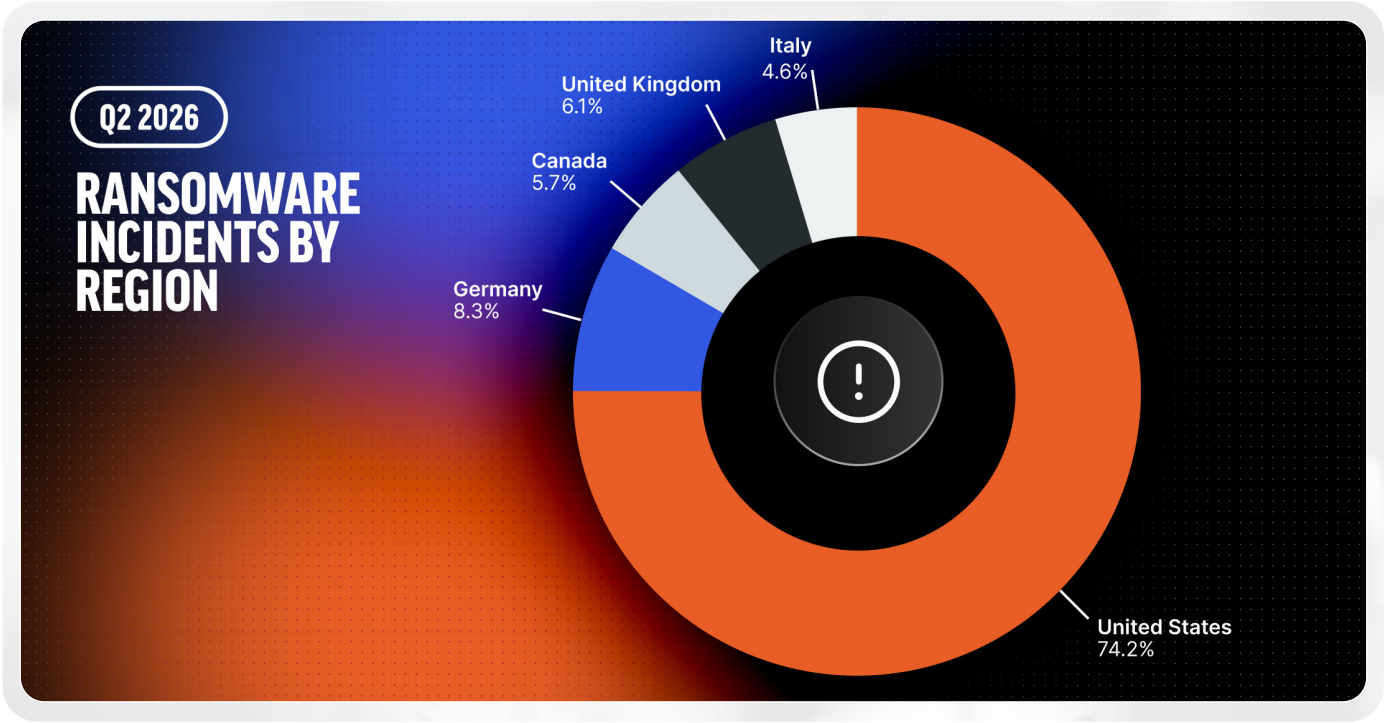
Active adversary trends and statistics

Popular incident techniques:

Attackers consistently focus on escalating privileges and moving deeper into the network once an initial foothold is established, with a high prevalence of post-exploitation activity. Credential harvesting, abuse of Remote Management Tools, and exploitation of public-facing software remain popular.

Ransomware activity:

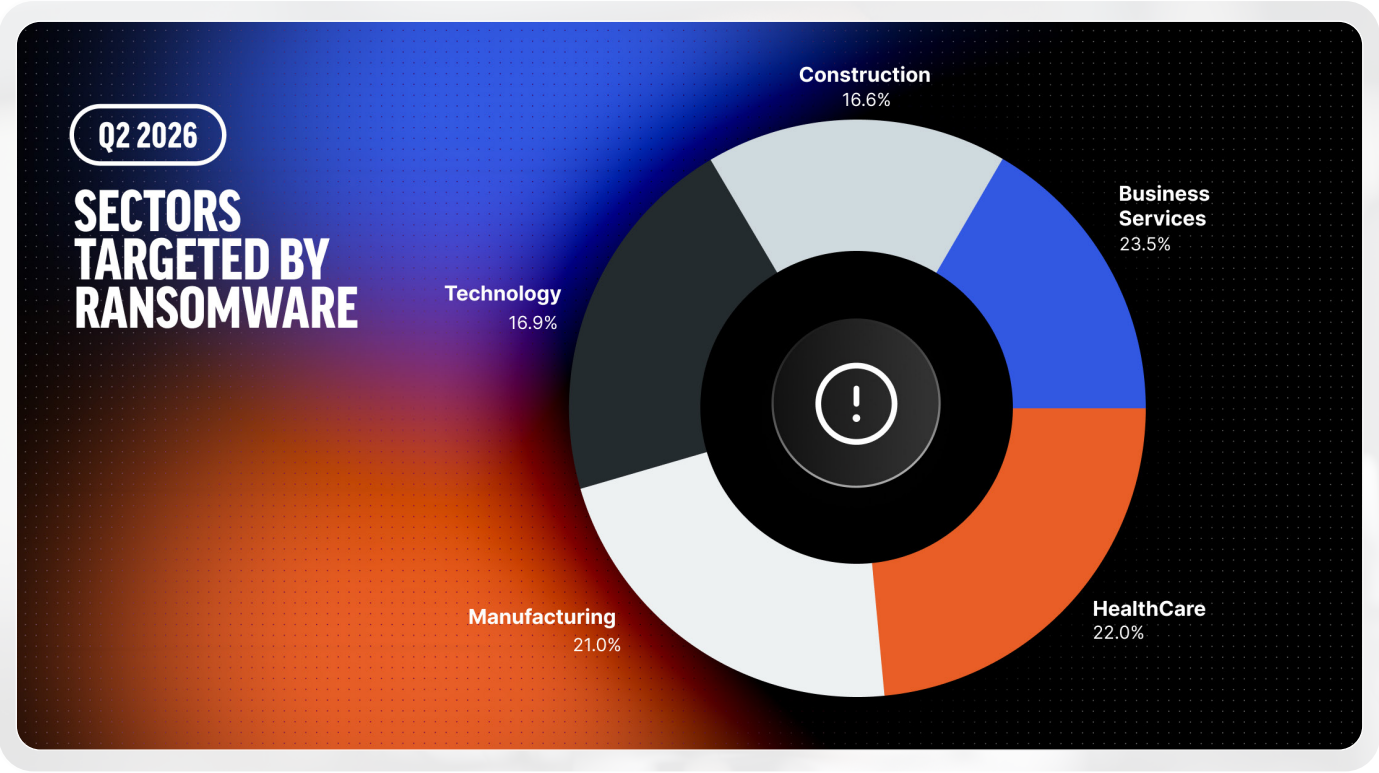
US organizations remain the ransomware epicenter — 881 listed victims across Q2 2026, roughly 9× the #2 country, Germany, with 99. But the quarterly top 10 now includes India (35) and Thailand (15). Having two non-western countries in the leaderboard is evidence that affiliate programs are actively expanding beyond English-speaking targets. Security teams in APAC can no longer treat ransomware as mainly a US/EU problem.



Labs and IR services

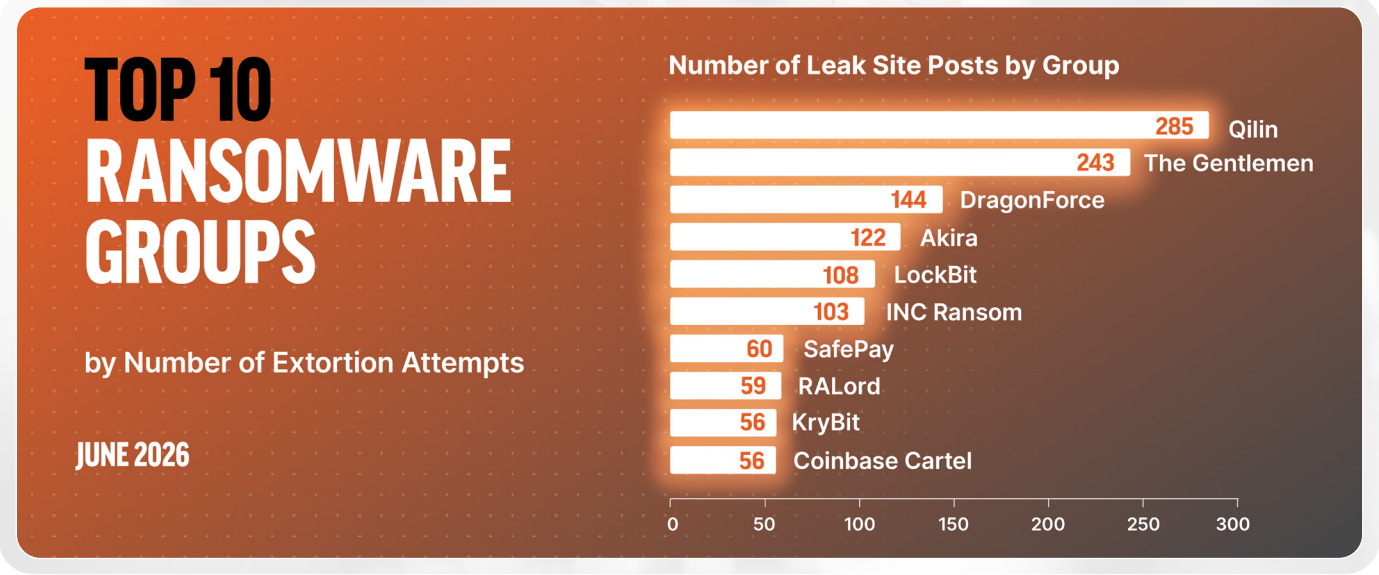
Rapid7 Labs and our Incident Response services team observed the below in Q2 2026:

- The top 3 ransomware groups of Q2 were Qilin (263 leak posts), The Gentlemen (230), and DragonForce (141).
- Fake CAPTCHA and ClickFix social engineering techniques make up 31.8% of observed IR incidents, impacting critical sectors such as healthcare, manufacturing, and communications & media.
- We have observed social engineering in Microsoft Teams becoming increasingly popular, highlighting a shift from phishing emails to trusted internal collaboration channels.



Dominant MDR trend themes

- **Device Code Phishing and Authentication Broker Abuse**
- **Credential Dumping:** Local Security Authority Subsystem Service (LSASS) and Mimikatz Persistent Presence
- **Ransomware Activity:** Black Cat, Black Basta, and SentinelOne Detections



DARK WEB INTELLIGENCE: UNDERGROUND FORUM SIGNALS

Underground economy status

Exploit trading on TOR and clearnet forums remains as popular as ever, with traditional vulnerability listings sitting alongside AI-assisted exploit discovery or AI tooling as an attack surface.

CVE stats:

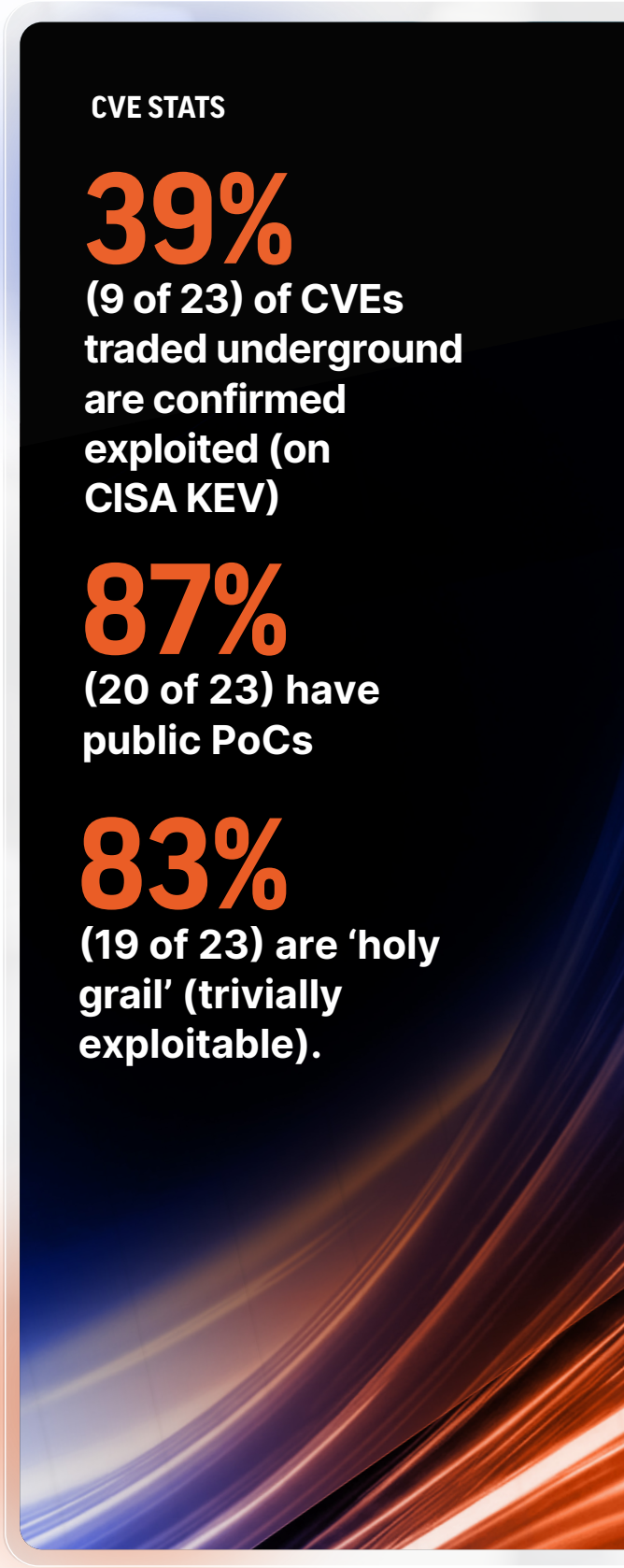
39% (9 of 23) of CVEs traded underground are confirmed exploited (on CISA KEV); 87% (20 of 23) have public PoCs; 83% (19 of 23) are 'holy grail' (trivially exploitable).

Popular vendor targets:

Fortinet is referenced in 1 in 16 forum post listings (7 in total).

Recommended actions

- Inventory and patch internet-facing edge appliances — SSL-VPN, RDP gateways, web servers.
- Rotate credentials and enforce phishing-resistant MFA on all remote-access paths.
- Cross-reference CVEs surfacing in disclosure spikes against your asset inventory.



SO WHAT DOES THIS MEAN?

The second quarter of 2026 makes one thing painfully clear. The era of the wait and see patch cycle is officially over. Disclosure volume is outrunning any team's capacity to triage it, and the flaws attackers use most need no credentials and no clicks. Adversaries are simply not waiting for organizations to sit around and debate maintenance windows or who owns what. Instead they are actively hunting for the path of least resistance. That could be an unauthenticated edge appliance, a vulnerable identity path, or even a socially engineered trap inside a trusted Microsoft Teams chat.

This is not some hypothetical AI driven vulnpocalypse. It is a highly operationalized landscape where threat actors are aggressively automating their discovery processes. The practical response isn't to chase every new vulnerability — it's to shrink the exposure that is actually reachable. The board will ask how much reachable, exploitable exposure are we carrying? Answering that question with evidence is indicative of a preemptive security program. Attackers have successfully compressed the time it takes to strike, so defenders must now forcefully compress the space in which those attackers can operate.

ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our website, check out our blog, or follow us on LinkedIn or X.