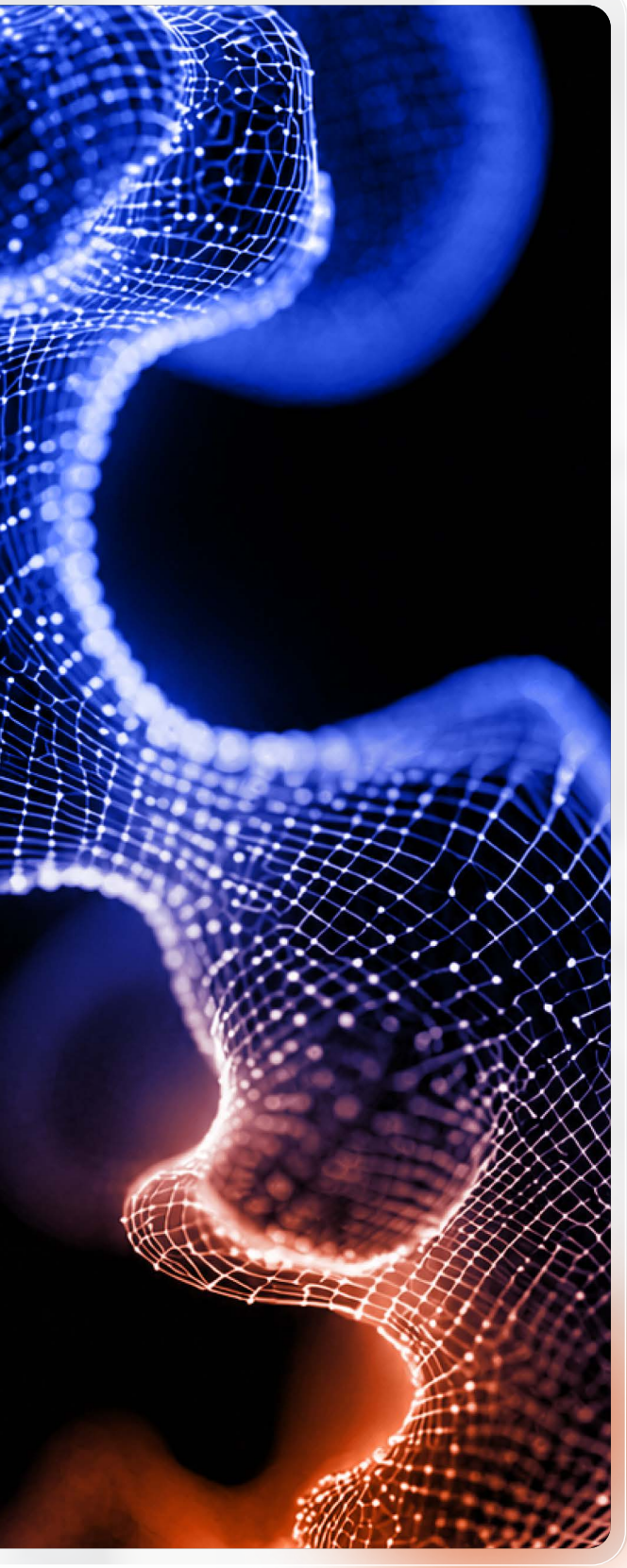
RAPID7

Q1 2026 THREAT LANDSCAPE REPORT

From Rapid7 Labs

RESEARCH REPORT

INTRODUCTION



Welcome to our latest Quarterly Threat Landscape Report, and one that, based on the amount of activity, reveals an environment that is particularly challenging for security practitioners to navigate. In this edition, we have witnessed significant geo-political changes with continued conflict across multiple geographies. Combined with the exploitation of critical vulnerabilities only increasing, it is fair to say that the need to gather actionable intelligence is more important than ever. This is the objective of this report: to provide a summary of the key insights necessary to prioritize resources and ensure security controls remain up to date with the emerging capabilities of well-funded threat actors.

As ever, our focus remains across the breadth of three key intelligence vectors: the emerging vulnerability intelligence findings, traditional threat intelligence (tracking both criminal and APT activity), and digital risk intelligence, which tracks dark web and underground forums.

As we consider this quarter, the current escalation of military activity in the Middle East has consumed the majority of headlines. Whilst this is understandable, it is important to note that there remains a very persistent criminal ecosystem that continues to exploit critical vulnerabilities, buoyed by earnings from illicit activities. What this means is that we are now seeing over 50% (20 out of 39) of the vulnerabilities actively exploited in the wild during Q1 fitting the zero-click/network-facing profile whereby these are network exploitable, no authentication, and no user interaction required.

Of course not all the activity this quarter is an escalation, as we detail the law enforcement actions disrupting criminal forums and what this likely means. As ever, we remain committed to the collection, curation, and delivery of actionable intelligence to our customers, as well as the infosec community, through multiple channels including our comprehensive open source portfolio.

As ever, please stay informed and safe.

Raj Samani
SVP, Chief Scientist

KEY REPORT TAKEAWAYS:

KEY TAKEAWAY 1

Vulnerability weaponization accelerated

Attackers are heavily prioritizing zero-click, network-facing vulnerabilities to achieve immediate, unauthenticated remote code execution. Furthermore, active exploitation is heavily preceded by massive spikes in social chatter, making public discourse a critical early warning indicator.

KEY TAKEAWAY 2

Geopolitical escalation as a catalyst

Cyberspace is increasingly being utilized as a direct instrument of state power. Q1 2026 saw highly synchronized cyber-military operations in the Middle East and a blurring of the lines between state actors and proxy hacktivist groups orchestrating disruptive campaigns against critical infrastructure.

KEY TAKEAWAY 3

Decentralization of the underground

Coordinated global law enforcement operations (such as the seizures of RAMP and LeakBase, alongside the BreachForums leak) have severely disrupted the cybercriminal economy. While this creates immediate friction for threat actors, it is forcing a migration toward decentralized, highly volatile platforms.

38%

of initial access vectors came from vulnerability exploitation and

50%

of those were zero-click, network-facing vulnerabilities.

Strategic shift

The primary exposure now lies less in immediate disruption than in undetected persistence and the potential activation of that access during periods of geopolitical tension.

GEOPOLITICAL ESCALATION

Regional threat overview

Q1 2026 marked a clear intensification of cyber activities within geopolitical dynamics, reflecting a structural shift toward cyberspace as a central instrument of state power.

Middle East escalation:

Following the February 28 strikes, cyber operations were closely synchronized with military actions between the US, Israel, and Iran. Iranian state-aligned actors targeted government infrastructure, industrial control systems, and financial services in the Middle East and US.

Russian and Chinese campaigns:

Russian cyber posture emphasized scalable access and intelligence collection by targeting network infrastructure, including routers and DNS systems. China sustained its long-term cyber espionage strategy, focusing on telecommunications, government communications, and political institutions.

THE VULNERABILITY INTELLIGENCE AND EXPLOIT LANDSCAPE

Critical exploit tracking

Q1 2026 saw a shift in emphasis within vulnerability exploitation.

Exploitation and public chatter:

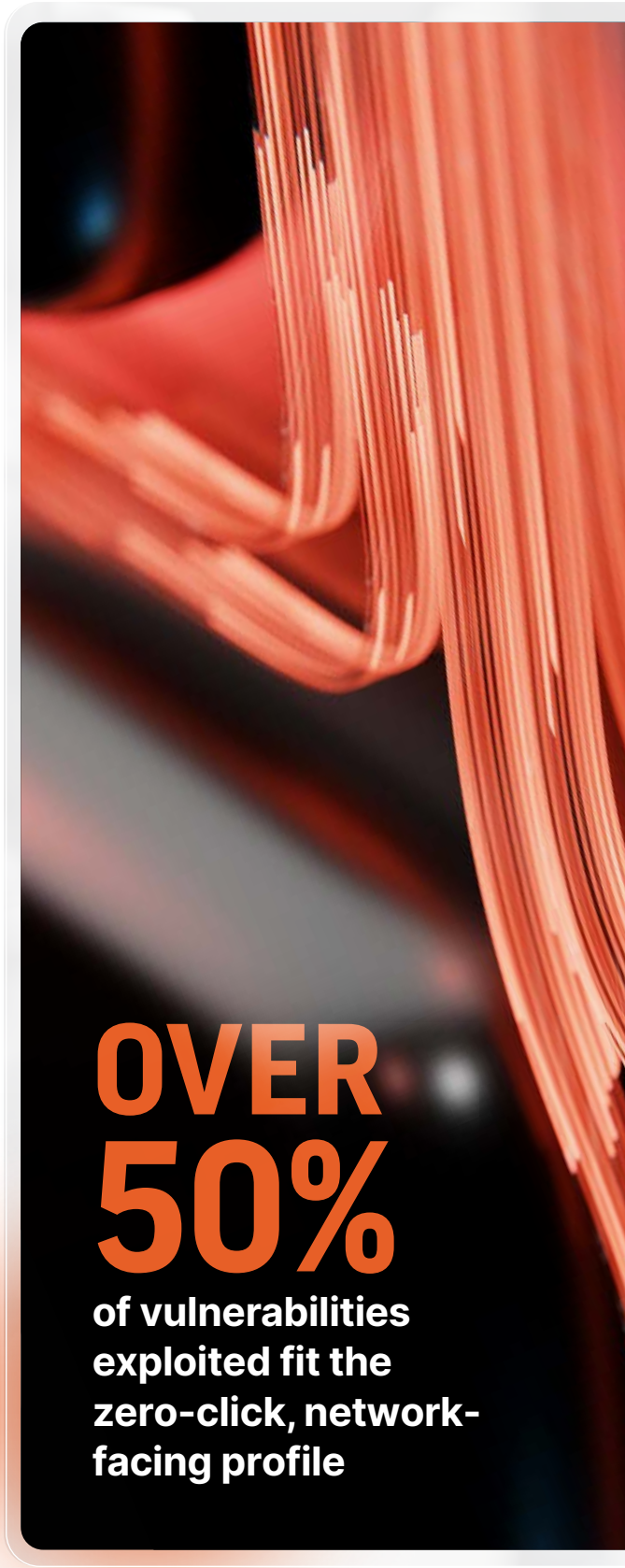
In Q1 2026, an exploited vulnerability averaged 1.8 million chatter hits — or those who have seen discussion of the exploitation — across blogs, forums, and social media. This is a massive acceleration compared to Q1 2025.

The “Holy Grail” vulnerability:

Over 50% (20 out of 39) of the vulnerabilities actively exploited in the wild during Q1 fit the zero-click, network-facing profile (network-exploitable, no authentication, no user interaction).

Rise of SQL Injection:

SQL Injection (CWE-89) emerged as the #1 most exploited vulnerability type in Q1 2026, overtaking OS Command Injection.



THREAT ACTOR ACTIVITY

Active adversary profiles

The landscape is driven by the rise of loosely coordinated, state-aligned cyber ecosystems and persistent pre-positioning.

State-aligned hacktivism:

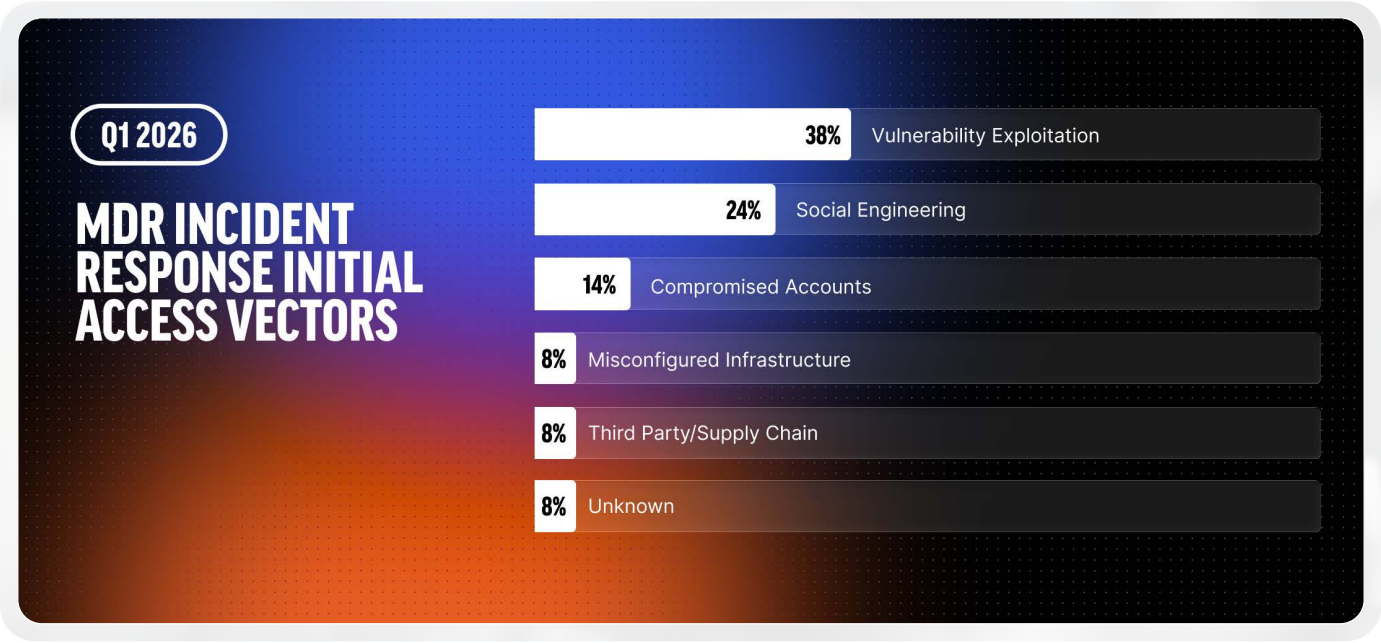
Iranian actors like MuddyWater, Handala, and APT IRAN conducted reconnaissance and exploitation against critical sectors. Pro-Russian hacktivists, such as NoName057(16), supported these operations with DDoS attacks and defacements against Western and allied infrastructure.

Financially motivated actors:

North Korea continued to integrate cybercrime into state strategy, leveraging large-scale cryptocurrency theft and supply chain compromises.

Ransomware affiliate evolution:

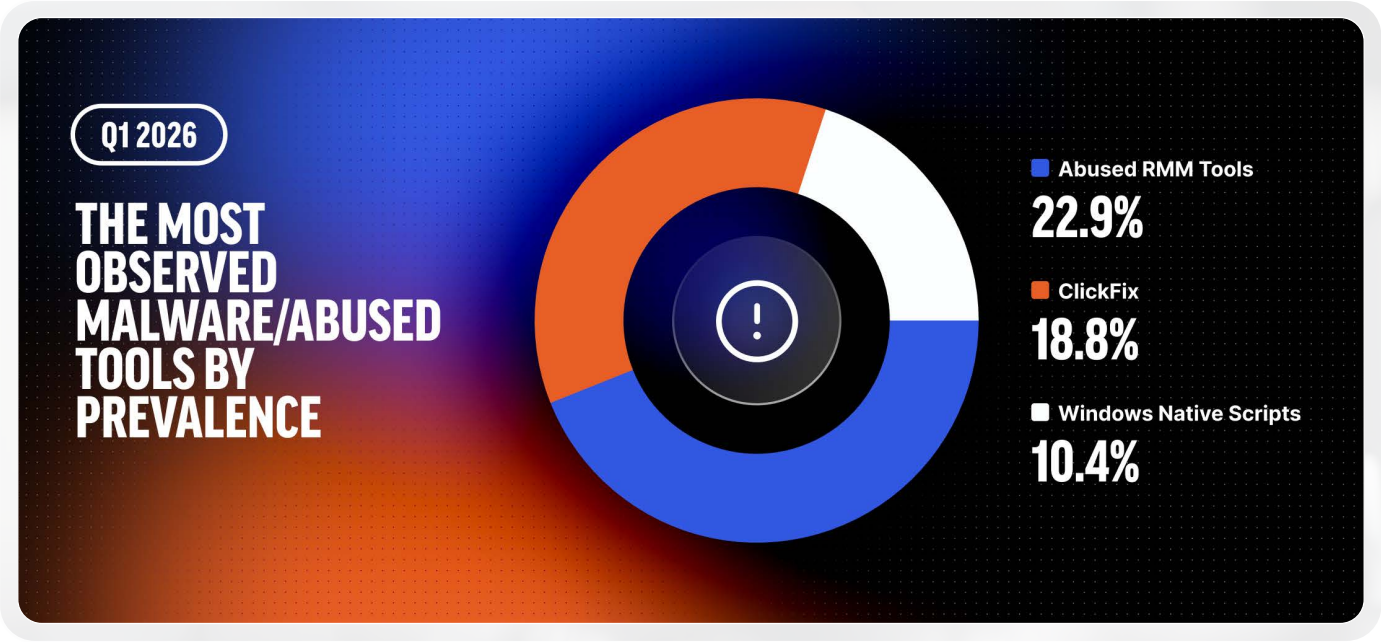
In response to the dismantling of major ransomware-as-a-service (RaaS) hubs like RAMP, displaced affiliates are adopting highly decentralized operational models and accelerating rebranding efforts. Tactically, these groups are increasingly pivoting toward “pure extortion” — weaponizing zero-click edge vulnerabilities to achieve rapid initial access and data exfiltration, effectively bypassing the overhead and detection risks associated with deploying traditional encryption payloads.



Labs and IR services

Rapid7 Labs and our Incident Response services team observed the below in Q1 2026:

- The top 3 ransomware groups of Q1: Qilin (357 leak posts), The Gentlemen (206), and Akira (174).
- The most observed malware/abused tools by prevalence: abused RMM tools (22.9%), ClickFix (18.8%), Windows Native Scripts (10.4%).



TTP shift analysis

The blurring of boundaries between state and non-state actors reduces the effectiveness of attribution-driven response models. Resilience now depends on the ability to constrain lateral movement and detect weak indicators of compromise over time.

DARK WEB FORUM DISRUPTION AND LAW ENFORCEMENT FRICTION

Underground economy status

Q1 2026 represented a significant inflection point for international law enforcement efforts, marked by coordinated operations that dismantled key dark web infrastructures.

Forum breaches:

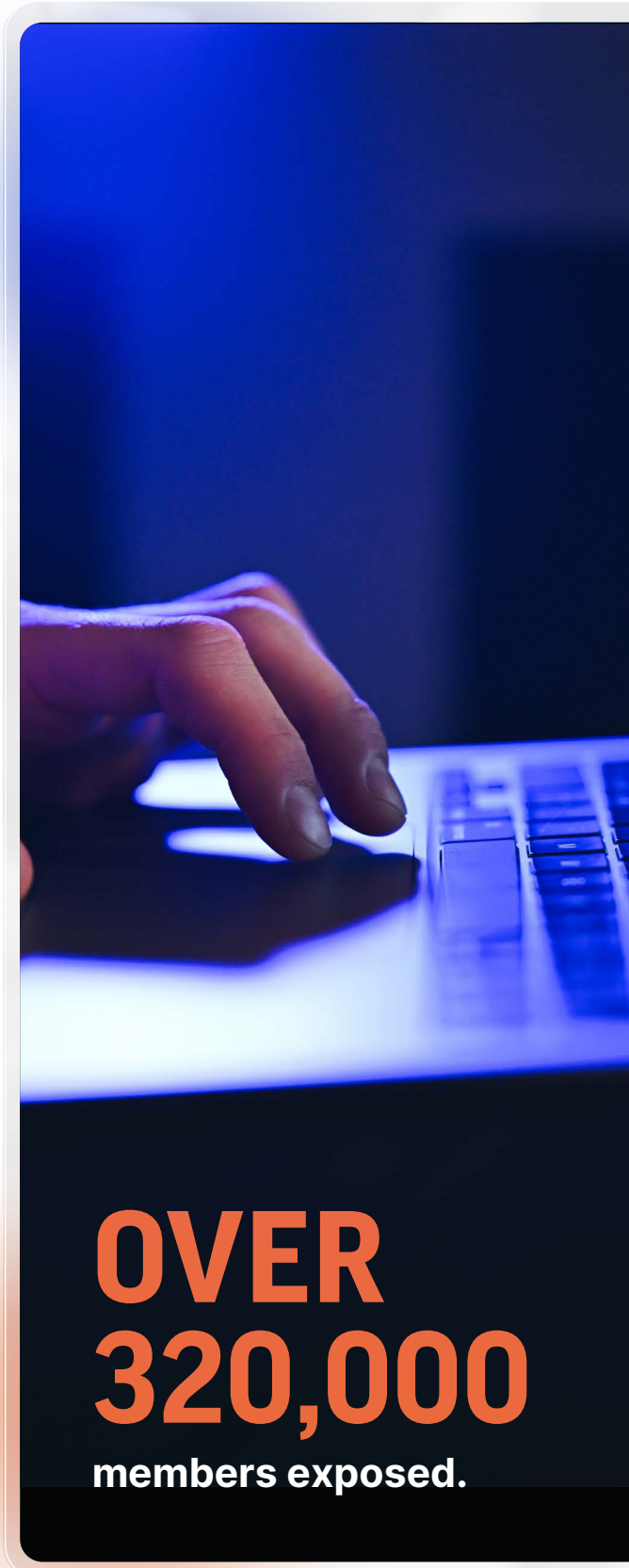
A major disruption occurred in January with the BreachForums data leak, which exposed the records and PGP keys of over 320,000 members.

RaaS and market seizures:

The U.S. FBI and DoJ seized RAMP, neutralizing a primary center for RaaS recruitment. Furthermore, a 14-country coalition executed Operation Leak in March, resulting in the seizure of the LeakBase credential marketplace.

Strategic forecast

These law enforcement interventions have significantly decentralized the cybercriminal ecosystem, increasing operational difficulty and internal distrust. CISOs should capitalize on this period of regrouping to accelerate security modernization projects, particularly around strengthening defenses against RaaS operations.



SO WHAT DOES THIS MEAN?

Taking the larger view of major incidents that occurred in Q1 2026, it is clear that waiting to react to threats is no longer enough — even trying to predict the next attack falls short. Attackers are turning zero-click vulnerabilities into weapons almost instantly, with the window to fix these issues growing vanishingly small.

Bad actors are launching attacks much faster than security teams can patch their systems. Because of this, adopting a truly preemptive security strategy is imperative. Teams cannot afford to sit around waiting for the next alert or rely on outdated snapshots of our network risk. We as a security community have to actively fix the underlying conditions that make attacks possible in the first place. This means continuously managing our weak spots and cutting off the paths attackers use most often, like user accounts with too much access and exposed edge devices.

When we combine this preemptive approach with active threat hunting and response, our security teams stop playing catch up. Instead, they can anticipate threats, focus on what matters most, and stop attackers long before real damage is done. At the end of the day, true resilience is about neutralizing threats at the speed they happen and — more and more — moving and operating at a preemptive pace. This will enable security teams to keep their businesses running smoothly without missing a beat.

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.