

QUARTERLY THREAT LANDSCAPE REPORT

Q3 2026

RESEARCH REPORT

RAPID 7

QUARTERLY THREAT LANDSCAPE REPORT

Q3 2026 has shown that attackers exploit new high-severity vulnerabilities in an average of just three days.

79%

Holy grail flaws

Of exploited vulnerabilities rated 7-10 CVSS required no authentication and no user interaction (34 of 43)

55

Government incidents

Government-sector ransomware incidents from the top Q3 countries

1,112

U.S. victims

Ransomware leak-site listings in the U.S. - roughly 8x Germany

41

dark web posts

Advertising RDP or network access; access-for-sale listings dominated the quarter

INTRODUCTION

WELCOME TO DAY 3

If you only keep one number from this report, make it 3. That's the average time between a new high-severity vulnerability going public and someone using it against somebody else. Not three weeks. Not "at the next change window." Three days. And 71% of all the exploitation we tracked landed inside the first seven. So if your patch cycle still has the word "monthly" in it, congratulations: It's perfectly calibrated for an adversary who stopped existing a while ago.

On the ransomware side, The Gentlemen and Qilin finished in a near photo finish, 342 versus 339 leak-site posts, before the field falls off a cliff to 99 for INC Ransom. The U.S. alone accounts for 1,112 listings, roughly eight times Germany, and in the government sector its share among the top ten countries jumped from 33% to 45%. Group names come and go like startups in a hype cycle. The tradecraft stays. Meanwhile on the underground forums, 41 of 63 posts were someone selling a way in, and the "exploits" on offer were mostly last week's advisories in a fresh jacket. No zero-day apocalypse, just a very well-run retail market for your RDP.

Despite talk of AI agents running wild, this quarter's AI-related cases remain human-directed for both targets and objectives, with AI assisting in the tactical middle of the attack chain as opposed to acting autonomously.

Which brings us to what's different on our side this quarter. We announced the Rapid7 Intelligence Organization, built on a simple idea: The research, the incident response front line, and the underground monitoring shouldn't sit in separate rooms, nodding politely at each other in meetings. You'll see that in this report: The vulnerability data, the leak sites, the forums, and what our responders keep running into come together as one story instead of four. We've also given the website a new look and feel.

At some point "three days" stops being a statistic and becomes a design requirement.

Welcome to day three. You're already late.

FIVE SIGNALS THAT DEFINED Q3 2026

TAKEAWAY 1

Government-sector incidents are concentrated more heavily at the U.S. among the countries we tracked in the ransomware top 10, with the U.S. share making up 45% of 55 Q3 government-centric incidents.

TAKEAWAY 2

Q3 2026's APT and cybercrime landscape shows continuity at the technique level - command and scripting interpreter, credential theft, and remote-access exploitation remain the backbone of both espionage and criminal intrusions.

TAKEAWAY 3

Attackers are rapidly weaponizing vulnerabilities, **exploiting new CVEs in an average of just 3 days**. This speed is fueled by the fact that 79% of the quarter's exploited flaws were remote, unauthenticated "holy grail" vulnerabilities. With 71% of all active exploitation occurring within the first 7 days, traditional weekly or monthly patching cycles are fundamentally too slow for defense.

TAKEAWAY 4

Most underground posts selling, sharing, or discussing exploits referenced CVEs already in vendor advisories or CISA KEV within days of disclosure, indicating rapid commercial repackaging rather than a wave of genuinely novel zero-day sales.

TAKEAWAY 5

Ransomware activity reached a near photo finish

The Gentlemen led Q3 with 342 victims, narrowly ahead of Qilin at 339. The United States accounted for 1,112 listed incidents, with business services and manufacturing identified as the top targeted sectors.

Rank	Group	Incidents Claimed
1	The Gentlemen	342
2	Qilin	339
3	INC Ransom	99
4	DeadLock	98
5	KryBit	95
6	DragonForce	88
7	Akira	68
8	SafePay	65
9	Storm	60
10	Payouts King	59

NATION-STATE ACTIVITY ACROSS REGIONS AND INDUSTRIES

15

Tracked actors

Distinct APT and cybercrime actors tracked

107

T1059 events

Events mapped to Command and Scripting Interpreter

15

CVEs abused

CVEs actively abused by tracked actors

8%

AI operations

Tracked reporting citing AI as an operational component

DPRK-linked activity against South Korea

Rapid7 Intelligence disclosed a previously undocumented Linux toolkit - a backdoor named "ted" compiled directly into a trojanized HAProxy 2.8.12 build, paired with an SSH keylogger and a curl-based RAT ("curlRAT") - used against South Korean automotive and media organizations, likely since early 2025.



Groups of Note

Void Blizzard

A Russia-affiliated espionage actor whose publicly documented targeting has consistently centered on government organizations and law enforcement agencies, alongside defense, transportation, media, and healthcare, primarily in NATO member states and Ukraine. Government is a core, not incidental, target sector.

Operation C-Major

A Pakistan-linked espionage operation whose targeting has centered specifically on Indian government and military personnel since at least the mid-2010s, using spear phishing and mobile spyware against military and diplomatic staff. Its appearance in our CVE-to-actor tracking this quarter (CVE-2021-4034) is consistent with this actor's established government-focused profile. Government and military personnel are the defining target, not a side effect.

Top adversary techniques (MITRE ATT&CK)

107

Command and Scripting Interpreter

T1059 · observed

83

Obfuscated Files or Information

T1027 · observed

75

Masquerading

T1036 · observed

Sectors Actively Targeted

- Aerospace
- Defense
- Transport
- Govt/Administration
- Finance
- Energy
- Health
- Technology

AI moved from drafting assistance to an operational role inside a meaningful number of tracked Q3 campaigns, and fragmented, multi-session prompting is emerging as the primary way threat actors evade AI provider safeguards. Disclosure data from at least one major AI provider this quarter indicated that single-session malicious requests were refused at a high rate, but safeguards performed less consistently once the same objective was split across multiple smaller sessions - a technique used deliberately by threat actors in disclosed cases.

CRITICAL EXPLOIT TRACKING

All data below covers vulnerabilities rated 7-10 CVSS.

3

Days to exploitation

Average time from CVE disclosure to exploitation in Q3 2026

3

Days to KEV

Median time between public disclosure and appearing on the CISA KEV list

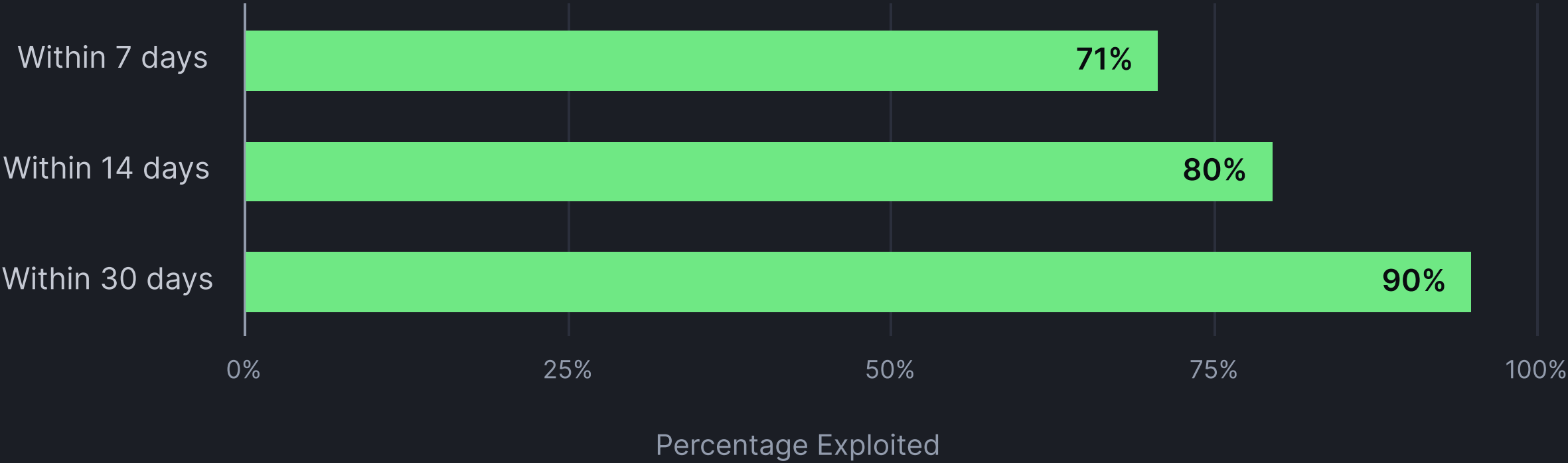
43

New exploited CVEs

Down 7% quarter over quarter, but still 19% higher year over year

Cumulative exploitation rate

71% of tracked exploitation occurred in the first seven days; 90% occurred within 30 days.



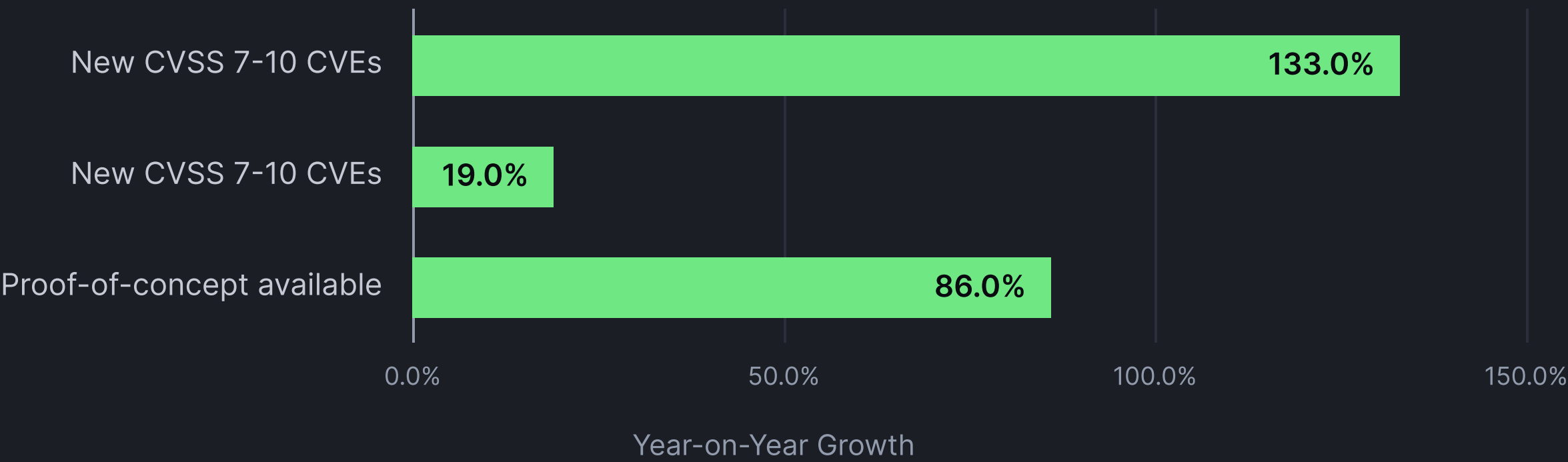
9.4%

PoC to exploitation conversion

One in ten proofs of concept becomes an active attack within 30 days.

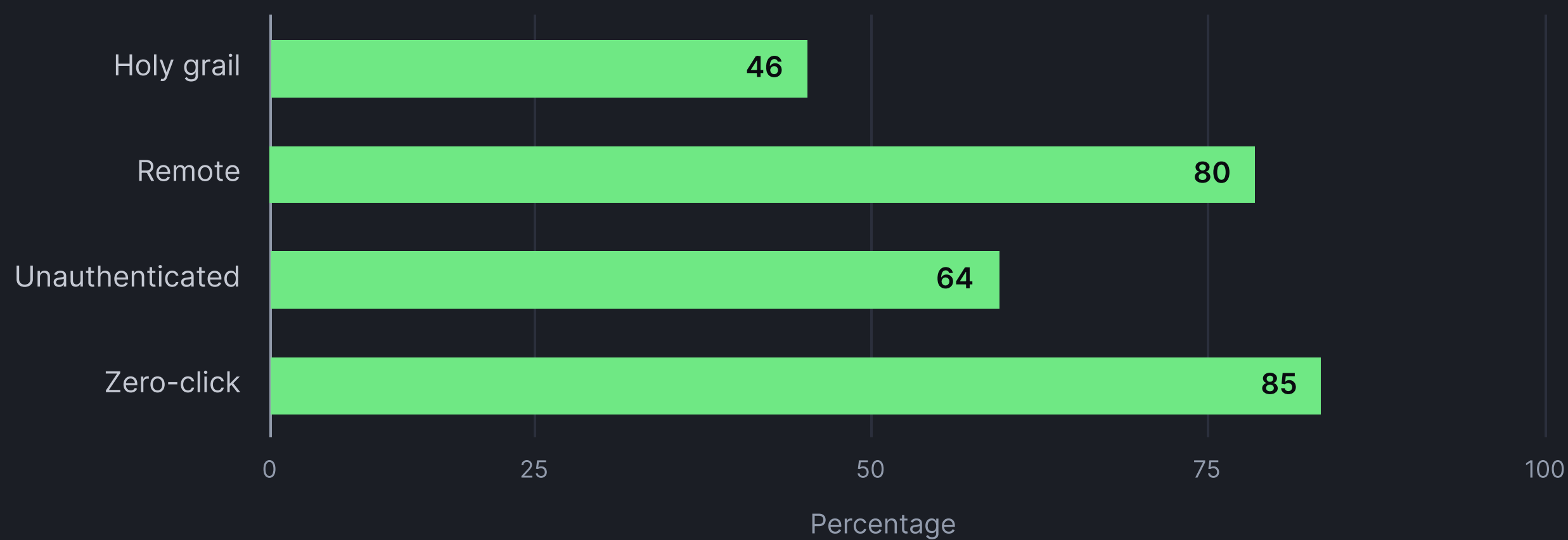
Year-on-Year Growth by Metric

Percentage growth compared with Q3 2025. Bar lengths are normalized to the 150% chart maximum.



Attack surface classification

Share of tracked CVEs with attacker-friendly characteristics.



Discovered vs. Actually Exploited

Each dot is one CVE. Grey dots were discovered. Green dots were successfully exploited.

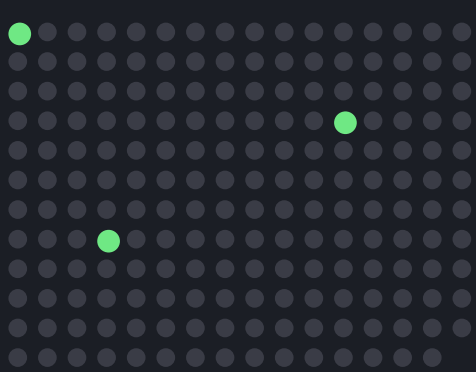


Remote Code Execution

18 exploited of 2,082 discovered

0.62% exploitation rate · the dominant impact type

2,930 CVEs total across four impact types. RCE accounts for 2,082.



Auth Bypass

3 of 191

1.57% exploitation rate · the highest of any impact type

Remote code execution accounted for 2,082 CVEs out of 2,930 across all four impact types. Eighteen of those RCE CVEs were exploited, while authentication bypass had the highest exploitation rate at 1.57% (3 of 191).

Vulnerability exploitation: CVE activity by actor

Our MISP dataset links 15 distinct CVEs to six tracked actors or clusters this quarter.

Actor	CVEs linked (Q3 2026)
APT31	CVE-2024-7344 , CVE-2025-0994 , CVE-2025-21042 , CVE-2025-3248 , CVE-2025-49704 , CVE-2025-49706 , CVE-2025-53770 , CVE-2025-53771
ENERGETIC BEAR	CVE-2008-4128 , CVE-2018-0171 (2 tracked events - highest single actor/CVE concentration in the dataset)
Lazarus Group	CVE-2025-49113
Operation C-Major	CVE-2021-4034
Sandworm	CVE-2025-20333 , CVE-2025-20362
Void Blizzard	CVE-2025-66376

Attackers aren't waiting. Map your external attack surface to find and fix exposures first.

[Explore Exposure Command](#)

THREAT ACTOR ACTIVITY

ACTIVE ADVERSARY TRENDS AND STATISTICS

Ransomware Activity

Government-sector incidents are concentrated further into the U.S. among the countries we tracked in the top 10. Among the top 10 reporting countries for government-sector ransomware, the U.S. share rose from 33% in Q2 (16 of 48 incidents) to 45% in Q3 (25 of 55 incidents). Qilin, The Gentlemen, KryBit, and SafePay are the most consistent government-sector operators across both quarters. The turnover among the remaining groups is notable - eight groups seen in Q2's government breakdown do not appear in Q3's, while seven new groups appear in Q3 that were absent in Q2.



Top Ransomware Groups

Rank	Group	Incidents Claimed	
1	The Gentlemen		342
2	Qilin		339
3	INC Ransom		99
4	DeadLock		98
5	KryBit		95
6	DragonForce		88
7	Akira		68
8	SafePay		65
9	Storm		60
10	Payouts King		59

Ransomware incidents by region

United States		60.4%
Germany		7.3%
Italy		5.3%
Canada		5.3%
United Kingdom		4.7%

Sectors targeted by ransomware

Business Services		17%
Manufacturing		16.1%
Healthcare		14.9%
Technology		10.8%
Construction		9.8%

Stop lateral movement before it becomes a breach. See how our 24/7 MDR team eliminates threats.

Explore MDR Services

UNDERGROUND FORUM SIGNALS

63 Underground posts Forum, market, and paste posts in Q3 2026	41 Access listings Posts advertising RDP or network access	14 Exploit posts Posts trading zero-days or exploits	10 Priority access Posts selling government or corporate access
---	---	---	--

Access-broker activity was the single largest category this quarter. Listings ranged from individual compromised accounts (bank logins bundled with “full” identity data for at least three major U.S. banks) to full enterprise footholds - an "Enterprise access with tailscale + RDP" listing bundling certified webmail access for a named footwear company.

Fourteen underground posts this quarter involved the sale, sharing, or discussion of exploits and zero-days. The majority referenced CVEs already in vendor advisories or CISA KEV within days of disclosure (for example, a September 25 forum thread on CVE-2026-94127, the F5 BIG-IP APM flaw disclosed September 22), indicating rapid commercial repackaging of known flaws rather than a wave of genuinely novel zero-day sales.

Recommended Actions

01 For public-sector defenders, the practical takeaway is that group-specific threat intelligence (for example, “watch for Group X”) has a shorter shelf life in this sector than the country- and technique-level patterns. Prioritizing detection and response capability against common ransomware tradecraft - rather than a static list of “the” government-targeting groups - is likely to hold up better across quarters.	02 None of this quarter's AI-related cases describe AI replacing a human attacker's judgment about targets or objectives - humans still chose what to attack and why in every documented case. What changed is how much of the tactical middle of an attack chain (technique selection, target triage, recovering from a failed step) can now run without a human present. For detection, this argues for monitoring AI API usage patterns from unexpected hosts and processes as a first-class telemetry source, not an afterthought.
--	--

SO WHAT DOES THIS MEAN?

Let's clear up a misunderstanding we already see in plenty of board decks: Two different apocalypses are being sold as one. The VulnDiscoveryPocalypse is real, because AI is finding flaws faster than anyone can triage them. The VulnExploitPocalypse isn't in our data. Yet. Only 43 vulnerabilities were newly exploited this quarter, fewer than the quarter before. But when attackers do show up, it takes them three days on average, and they shop in one aisle: remote, unauthenticated, zero-click. So treat it as a risk appetite conversation, not a patching one. A risk appetite you can't express in days of exposure is just hope with a budget.

Eight percent of the reporting we tracked cites AI as an operational component. In every documented case, a human still chose the target and the reason why. What the machine took over is the tactical middle: which technique next, who's worth the effort, what to do when step four fails. So if the middle of an attack no longer needs a human, what's left that is human is intent. Do you know what your adversary actually wants from you? Not the malware family. The want.

The clock isn't yours, and it was never going to be. You can complain about the pace or start designing for it. Only one of those makes for a better report next quarter.

A risk appetite you can't express in days of exposure is just hope with a budget.

Rapid7 Intelligence, Q3 2026

Research is only half the loop

Every Intelligence finding feeds the Command Platform, so the CVEs and detections here become prioritisation and hunts you can action.

[Explore the Command Platform](#)