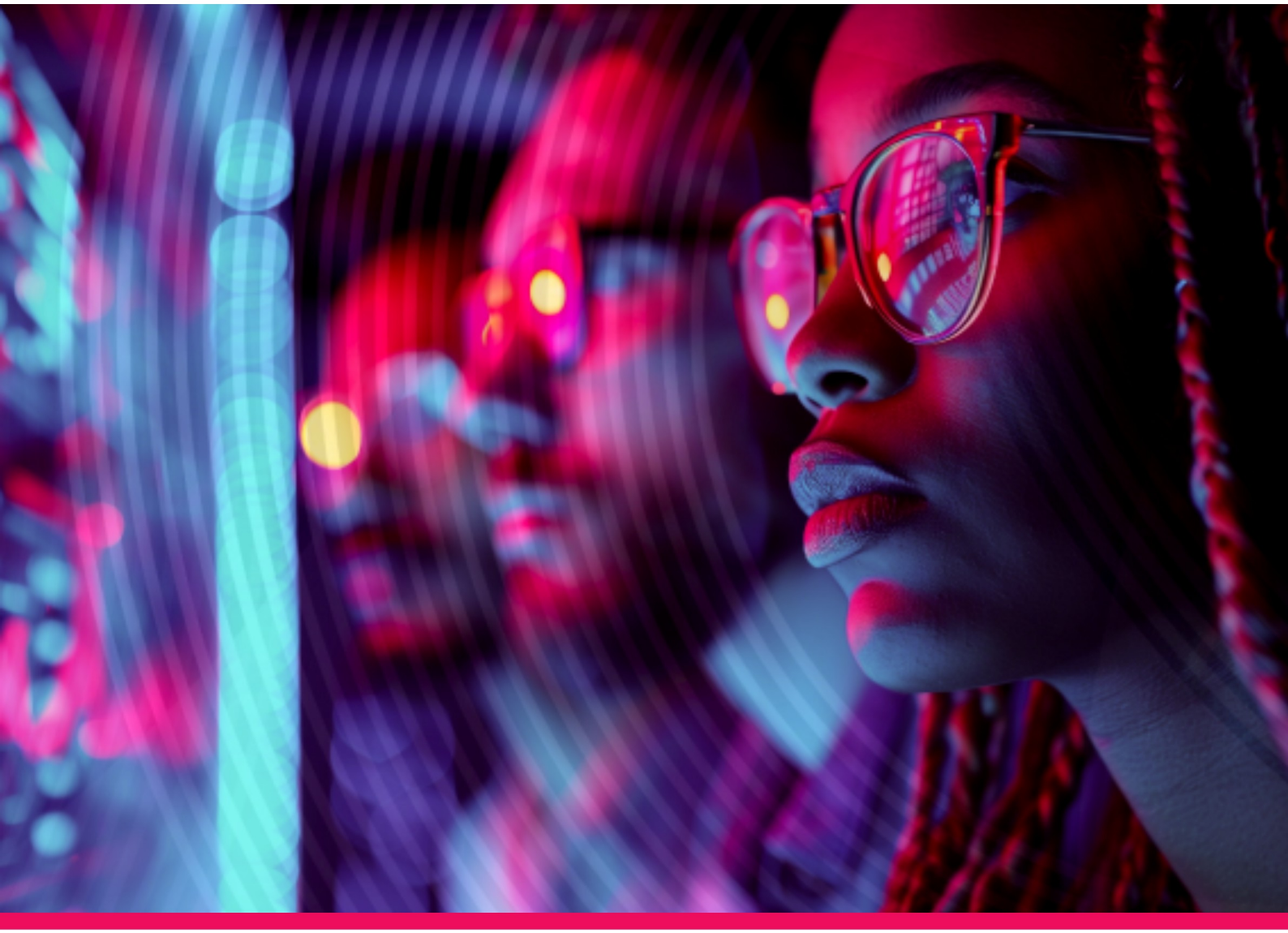


CHECK POINT EXPOSURE MANAGEMENT

The status of darknet forums: fragmentation, not decline

How law-enforcement disruption reshaped breach, data-leak and ransomware forums over the past two years, and what it means for visibility into the underground.

November 2026

01
FRAGMENTATION

02
VOLATILITY

03
REDUCED CONTINUITY

CONTENTS

Inside this report

01	**Executive summary**	**3**
02	**From Centralization to Fragmentation**	**4**
03	**Breaching Forums: A Community Without a Permanent Center**	**5**
04	**Ransomware forums: Fragmentation of the Russian-Speaking Underground**	**9**
05	**The New Underground**	**10**
06	**About Check Point Exposure Management**	**11**
07	**Contact us**	**12**

+15.3%

Average monthly breaches observed, from 273 before April 2025 to 315 after

Source: Figure 4

–28.1%

Average weekly initial access broker posts, from 471 before the XSS seizure to 339 after

Source: Figure 5

2 years

Of forum activity analysed across breach and ransomware communities

Source: Figures 3 and 6

The central development is fragmentation rather than decline

Cybercriminal forum activity remains substantial, but the communities producing it are increasingly distributed across unstable and sometimes competing platforms.



OVERVIEW

Executive summary

During the past two years, the cybercriminal forum landscape has undergone a period of sustained disruption. Law-enforcement operations, administrator arrests, seizures, internal disputes, and repeated shutdowns have weakened several communities that previously served as relatively stable gathering points for cybercriminal actors.

However, these disruptions have not eliminated the communities that depended on them. Instead, activity has increasingly dispersed across competing forums, successor platforms, clones, and newly established communities.

This trend is particularly visible following disruptions to major forums. Rather than one clear successor absorbing the displaced community, multiple platforms frequently emerge or expand simultaneously. Some achieve temporary momentum before declining again, while others establish smaller but more persistent communities.



Figure 1: Seizure banners for BF and XSS

What weakened the forums

Law-enforcement operations, administrator arrests, seizures, internal disputes and repeated shutdowns.

In the last two years, this transition could be seen in the forums' activity. Earlier periods are characterized by substantially greater concentration around a limited number of forums, while later periods show activity distributed across a broader and more volatile collection of platforms. Individual forums can still become dominant for short periods, but that dominance appears increasingly temporary.

The same pattern is visible within ransomware-oriented communities. Enforcement against established Russian-speaking forums has disrupted long-standing gathering points, while newer or smaller communities have attempted to fill portions of the resulting gap. Established forums such as Exploit remain relevant, but the broader ecosystem increasingly lacks a single venue capable of replacing the role previously occupied by major communities such as XSS or RAMP.

CHAPTER 01

From Centralization to Fragmentation

For much of the previous decade, cybercriminal forums benefited from network effects. Reputation systems, established administrators, escrow services, long-standing user identities, and accumulated marketplace relationships encouraged actors to congregate around a relatively small number of trusted communities.

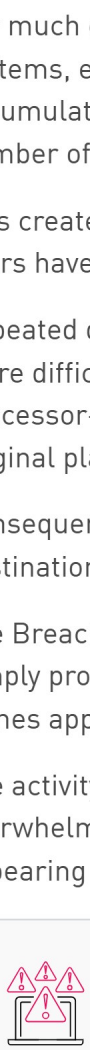
This created recognizable centers of gravity within different parts of the underground. The last two years have increasingly challenged that model.

Repeated disruptions have shortened the effective lifespan of major communities and made continuity more difficult. When a prominent forum disappears, the surrounding community must decide which successor—if any—to trust. Competing administrators may claim legitimacy, clones can replicate the original platform's appearance, and alternative forums can try to attract displaced users.

Consequently, the disappearance of a major forum increasingly produces several competing destinations rather than a single replacement.

The BreachForums ecosystem illustrates this particularly clearly. Its repeated disruptions did not simply produce a linear sequence of replacement forums. Instead, different revivals and competing clones appeared at different points, creating overlapping claims to the same broader community.

The activity seen reinforces this interpretation. Periods in which one BreachForums version overwhelmingly dominates are repeatedly interrupted by sharp contractions followed by activity appearing across alternative forums and successor communities.



Continuity is the real casualty

The important observation is therefore not the precise number of posts generated by each incarnation. It is that community continuity has become increasingly difficult to maintain through a single platform.



CHAPTER 02

Breaching Forums: A Community Without a Permanent Center

The breach and data-leak ecosystem provides perhaps the clearest example of this transition.

BreachForums once represented an unusually strong center of gravity for English-speaking breach trading and data-leak activity. Repeated disruptions weakened that position, but demand for the functions provided by the forum did not disappear. Instead, the surrounding community repeatedly reorganized.

BreachForums revivals attempted to reconstruct the original community, while competing clones and alternative forums sought to capture portions of the displaced audience. At the same time, platforms including DarkForums, PwnForums, the new RaidForums, Spear, and BHF provided additional destinations.

The resulting ecosystem is considerably more fluid.

This redistribution was seen very clearly when activity in BreachForums dropped; activity did not disappear from the wider landscape. Other communities grew, new forums emerged, and later versions of BreachForums regained part of the audience.

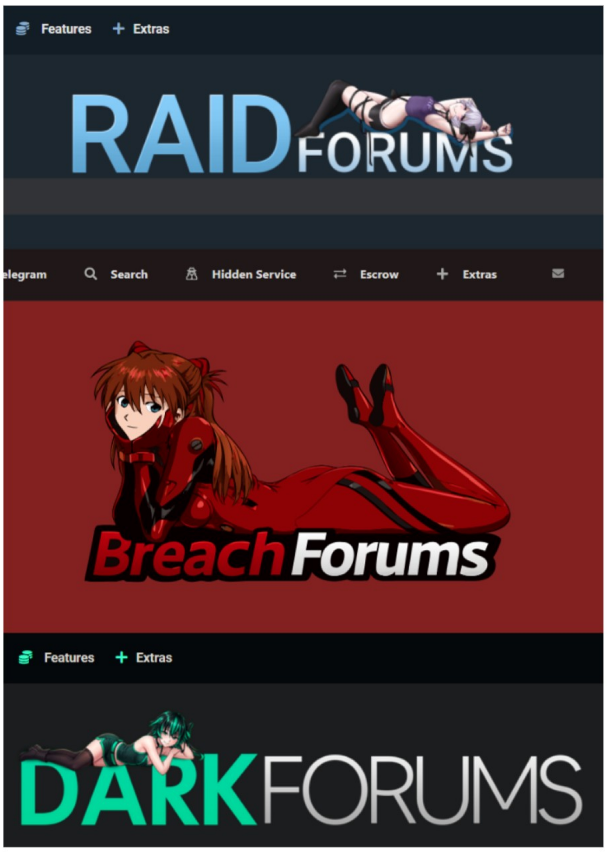
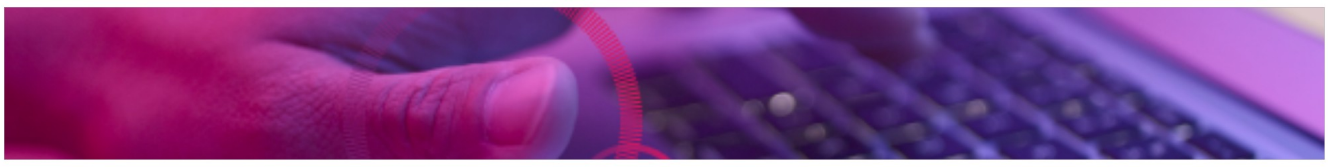


Figure 2: Current alternatives and their similarities.

DarkForums is especially illustrative. Its growth following disruption elsewhere in the ecosystem suggests that alternative communities can benefit significantly when established forums become unavailable. PwnForums and Spear similarly demonstrate that smaller communities can develop meaningful activity without necessarily becoming permanent replacements for the previous dominant forum.

This creates an environment in which leadership rotates between platforms rather than remaining permanently concentrated.



CHAPTER 02 · BREACH FORUMS

Where displaced activity went

Similar changes in activity do not, by themselves, prove that individual users moved from one forum to another. Even so, the wider pattern is consistent with displaced activity being spread across several competing communities.

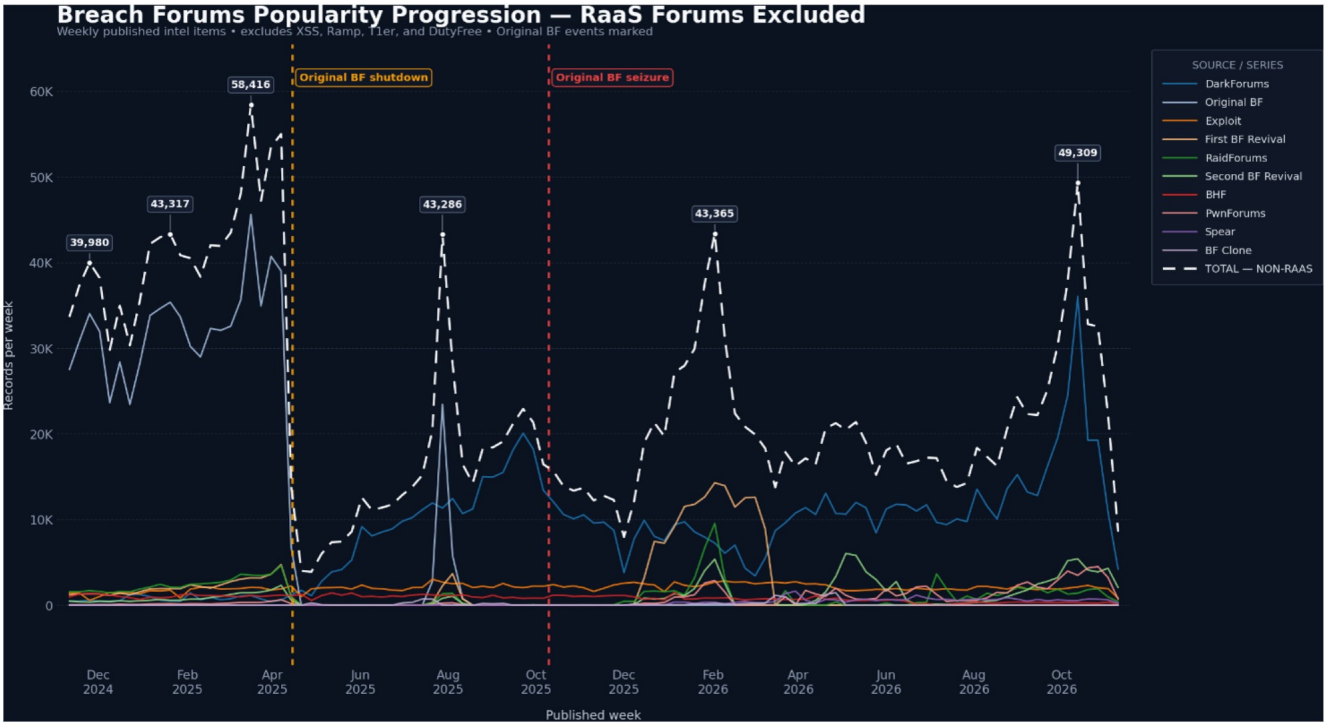


Figure 3: Breaching Forums activity in the last 2 years.



Platforms competing for the displaced community

DarkForums | PwnForums | The new RaidForums | Spear | BHF

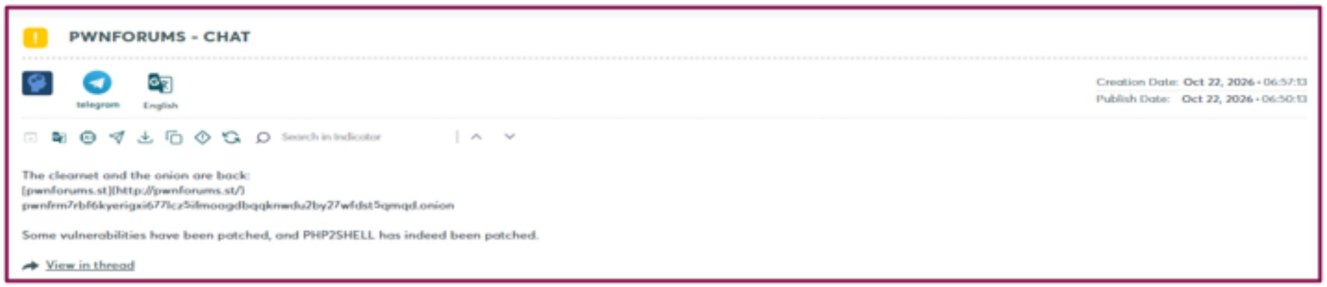
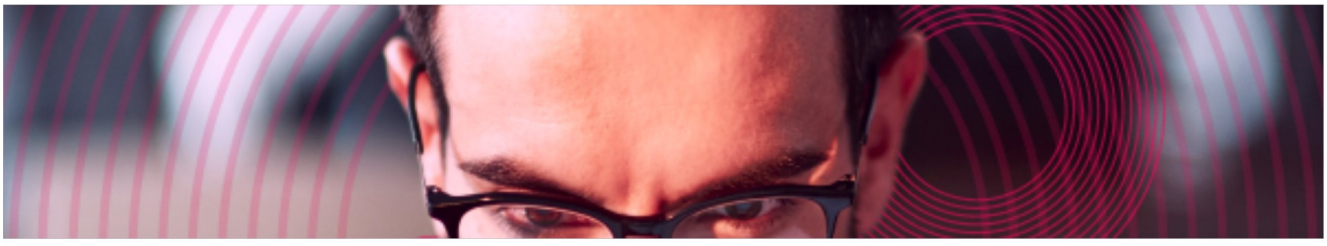


Figure 3b: PwnForums announces that its clearnet and onion sites are back and that PHP2SHELL has been patched (22 October 2026).



CHAPTER 02 · BREACH FORUMS

Fragmentation Without a Decline in Observed Breaches

Despite repeated disruption and the spread of activity across a growing number of alternative forums, the volume of observed breaches and data leaks did not decline. The Breaches Observed Over Time chart shows that average monthly volume increased from 273 incidents before April 2025 to 315 incidents from April 2025 onward—an increase of 15.3%.

This does not establish that forum fragmentation or the shutdown of the Original BreachForums caused the increase. It does, however, show that breach-related activity remained resilient as the community became more distributed. Disruption weakened individual centers of gravity, but it did not remove the underlying demand for trading breached data, publishing leaks, and promoting related activity.

These figures represent incidents seen, rather than a complete measure of all breach activity. The final November 2026 observation is partial and should not be compared directly with complete months; nevertheless, the broader two-year pattern supports the same conclusion: observed breach and data-leak volume did not fall as the forum ecosystem fragmented.

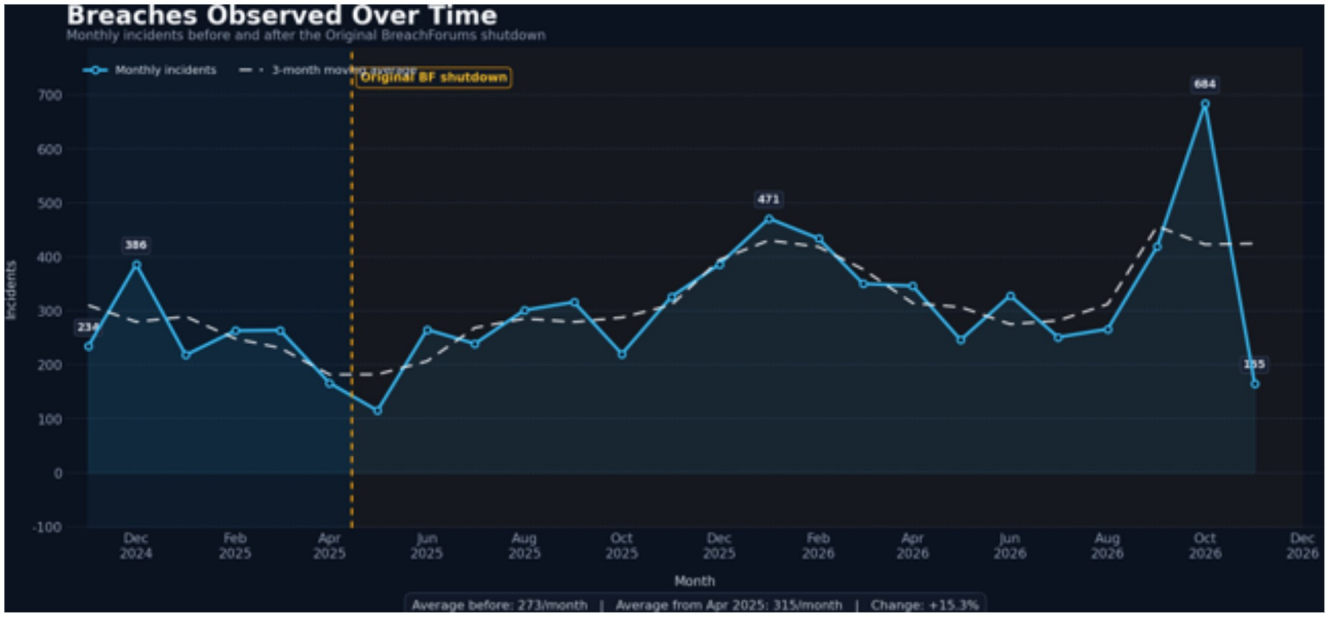


Figure 4: Activity of data breaches and leaks in the past 2 years.

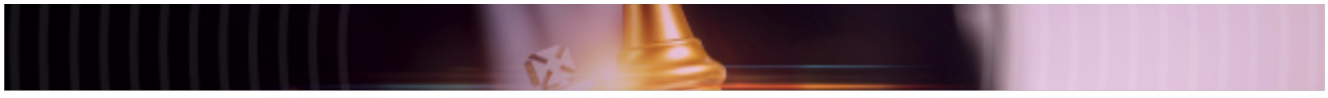
+15.3%

Increase in average monthly incidents seen after April 2025

Source: Figure 4

273 → 315

Average incidents per month, before and from April 2025.



CHAPTER 02 · BREACH FORUMS

Initial Access Activity Is Becoming Less Visible

The decline in initial access broker (IAB) posts following the seizure of XSS stands in contrast to the continued rise in ransomware activity. Across the monitored forums, average weekly IAB posts fell from 471 before the XSS seizure to 339 afterward, a decline of 28.1%. Yet ransomware incidents did not follow the same downward trend. This suggests that the fall in publicly visible access listings should not necessarily be interpreted as a comparable decline in the availability or trade of initial access.

One plausible explanation is that a growing share of this activity is taking place outside publicly visible forum marketplaces. Relationships between access brokers, ransomware operators, and affiliates may continue through private channels and established contacts, particularly once trust has already been built. In this environment, a broker may have less need to advertise access publicly if they already have reliable buyers or partners.

The divergence between declining forum posts and continued ransomware activity therefore highlights an important visibility gap. The market for initial access may not be disappearing so much as becoming less observable. While the available data cannot confirm where these transactions have moved, the continued pace of ransomware incidents suggests that reduced forum activity alone is not evidence of reduced access to compromised organizations.

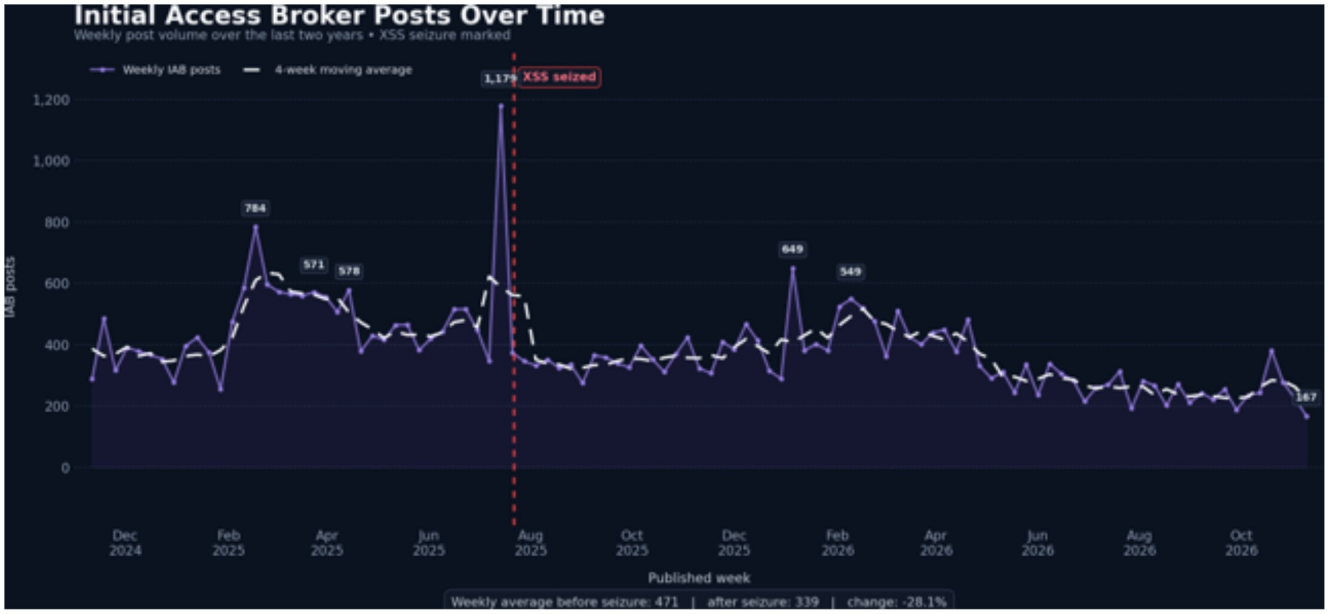


Figure 5: Activity of initial access posts in the past 2 years.

−28.1%

Drop in average weekly IAB posts after the XSS seizure

Source: Figure 5

471 → 339

Average weekly posts, before and after the seizure. A visibility gap, not necessarily a market decline.

CHAPTER 03

Ransomware forums: Fragmentation of the Russian-Speaking Underground

A similar process is occurring within the Russian-speaking cybercriminal ecosystem, although its structure and culture differ from the breach-focused community. Historically, established forums benefited from years of accumulated reputation and relationships between administrators, brokers, malware developers, access sellers, ransomware operators, and other participants.

This made communities such as XSS and RAMP particularly difficult to replace. Law-enforcement disruption therefore affects more than the availability of a website. It can disrupt the trust infrastructure surrounding the community.

The disruption of XSS and later pressure against RAMP contributed to an environment in which ransomware-related actors increasingly lacked an obvious central gathering point.

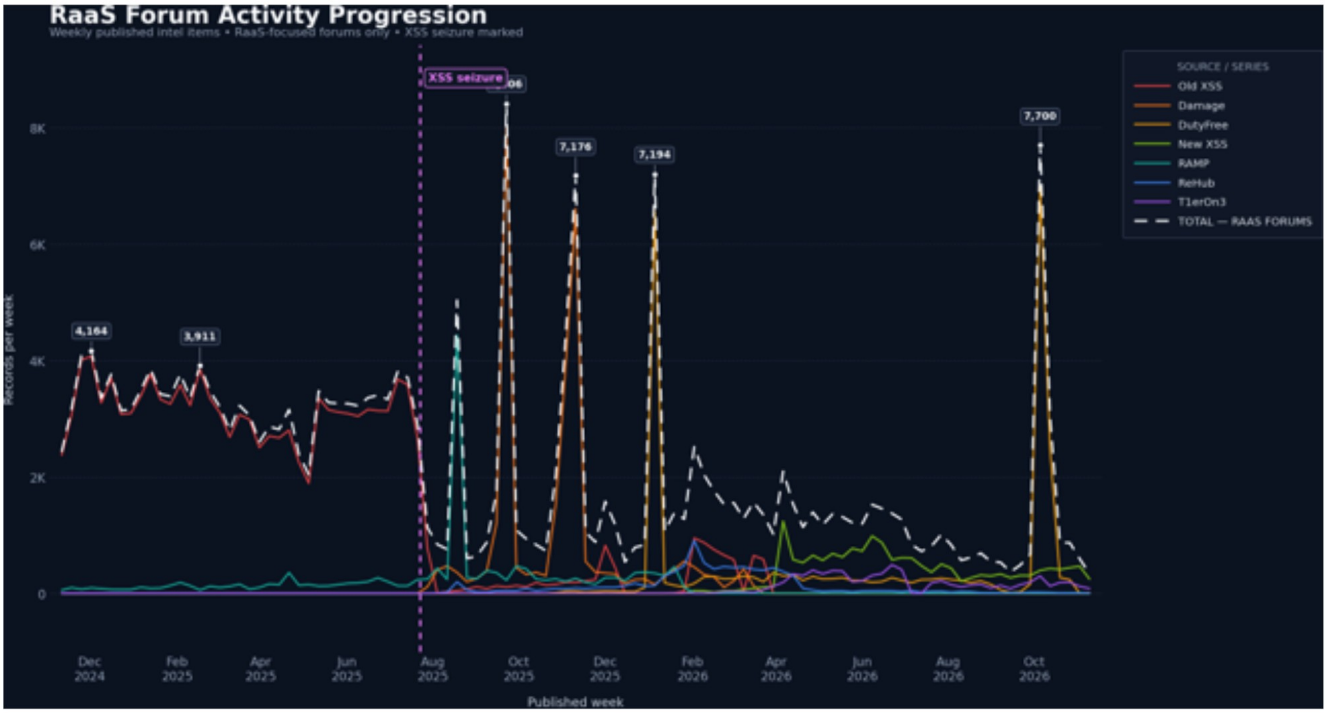


Figure 6: Ransomware-permitting forums activity in the last 2 years.



Newer venues are not direct replacements

Communities including DutyFree and T1erOn3 have attempted to occupy portions of this space, while established forums such as Exploit continue to provide continuity. None should automatically be interpreted as a direct replacement for the communities that preceded them.

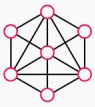
The activity data supports this distinction. Exploit demonstrates comparatively persistent activity across the last two years, while newer communities generally show smaller and more volatile levels of participation. XSS-related activity, meanwhile, illustrates the difficulty of recreating an established underground community after disruption.

> This suggests that technical replacement is considerably easier than community replacement. A new forum can be launched quickly; rebuilding reputation, relationships, and trust is much harder.

CHAPTER 04

The New Underground

By late 2026, the defining characteristic of the forum ecosystem is therefore not inactivity but instability. The underground still contains large and active communities, but fewer platforms appear capable of maintaining uncontested dominance for extended periods. Three characteristics increasingly define the environment:



FRAGMENTATION

Activity is distributed among more competing communities. A disrupted forum increasingly gives way to several destinations rather than one clear successor.



VOLATILITY

Venues can grow rapidly after disruption elsewhere, but prominence may be brief. Isolated spikes require validation before they are treated as organic growth.



REDUCED CONTINUITY

Successors can inherit branding without inheriting administrators, reputation histories, user identities or trust relationships.



Law enforcement has therefore had an important cumulative effect even when individual operations have not permanently removed the underlying criminal communities. Each disruption forces actors to rebuild relationships, establish new identities, evaluate competing platforms, and determine which administrators can be trusted. Over time, these repeated disruptions increase friction within the ecosystem.

Fragmentation also makes the underground harder to observe

Intelligence collection that previously depended on monitoring several dominant communities increasingly requires coverage across a larger and constantly changing collection of platforms.

About Check Point Exposure Management

Check Point's exposure management changes the game. We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit
checkpoint.com/exposure-management

Explore Exposure Management →



CHECK POINT

EXPOSURE MANAGEMENT



CONTACT US

ISRAEL
Tel: +972-73-226-4555
5 Shlomo Kaplan Street, 6789159

USA
Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800, Redwood City, CA 94065

SINGAPORE
Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1, Singapore 079120

PHILIPPINES
Tel: +63-2-8465-9200
Unit 2005, 20th Floor, Zuellig Building, Makati Avenue, corner Paseo de Roxas, Makati City 1223, Metro Manila

UK AND IRELAND
Tel: +44-20-7628-4211
85 London Wall, 4th Floor, London, EC2M 7AD

JAPAN
Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F, 1-2-8, Toranomon Minato-ku, Tokyo 105-0001

© 2026 Check Point Software Technologies Ltd. All rights reserved.