radware

Report

From Hackers to Founders: The 2026 State of the Underground Ecosystem

Exploring AI's Effect on Modern Threat Actors and Their Thriving Platforms

For more than a decade, underground hacker forums have been one of the most important stages where the cyberthreat landscape unfolds. These forums evolved from a small, unique community of amateur hackers into large marketplaces where less technically versed hackers (buyers) and more technically versed hackers (sellers) trade and interact. Despite numerous takedowns by Interpol and local authorities, many forums come back to life each time with a new address, better operational security (OpSec) and a more focused user base.

The recent Substack data breach (Figure 1) illustrates how a single post from a threat actor can affect a company's actions and media headlines.

February 2: A threat actor publishes Substack's 697,313 records

February 6: The CEO sends an email to customers confirming the data breach

Ongoing: The media follows and covers the story

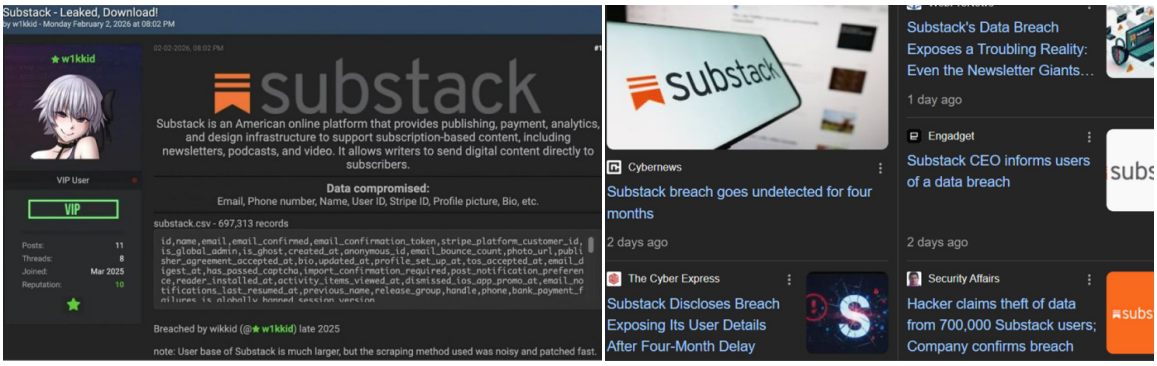


Figure 1:

Substack database published by threat actors in a deep web forum (source: Breachforums[.]bf), media headlines following the leak post (source: Google News)

But what do we really know about the places where anyone with a crypto wallet can buy anything from a phishing kit for Microsoft Office 365 and a virtual private server (VPS) to a breached database and a powerful bot script for less than $100?

Throughout January 2026, Radware's Cyber Threat Intelligence (CTI) team collected threads, posts, ads and profile information from **BreachForums[.]bf (BreachForums), Cracked[.]sh (Cracked)** and **Lolz[.]live (Lolz)**—three major deep- and dark-web forums popular among application threat actors. This research focuses on the following key aspects of the current threat landscape:

1. **Platforms:** Our traffic analysis review reveals threat actor details, including age distribution, how they reach the platform and which AI service they prefer.

2. **Threat Actors:** We discover the common threat actor types that typically lead forums and explore how AI hype influences hacker platforms and operations.

Table of Contents

Executive Summary

The 2026 cybercrime landscape is defined by a fluid form of resilience. Despite aggressive multinational law enforcement campaigns, including the multiple seizures of BreachForums and the dismantling of Cracked, the underground economy has not contracted. Instead, it has reorganized. Following the August 2024 arrest of Telegram's CEO and the platform's subsequent policy pivot, threat actors have conducted a massive reverse migration, fleeing social apps to re-establish entrenched positions in multiple deep-web forums.

Forum Dynamics

An analysis of 2.5 million monthly visits across three major hubs (Cracked, Lolz, and BreachForums), reveals a thriving ecosystem driven by a young demographic, with one in three visitors estimated to be between 18 and 24 years old. These communities have divided into three types of operational models:

- **The Fortress:** Cracked relies on 77% direct traffic, servicing a vetted, high-retention community of technical operators.
- **The Supermarket:** Lolz operates as a high-volume commercial hub, generating 40% of its traffic from organic search and catering to entry-level gamers and script kiddies.
- **The Brand:** BreachForums survives on its infamy, with significant organic traffic driven by public notoriety following media coverage of major leaks.

The AI Divide and "Vibe Coding"

Artificial intelligence adoption is not uniform across the underground; it is role-specific. While nearly 48% of Cracked users (developers and scripters) engage with AI tools like ChatGPT simultaneously, only 12% of BreachForums users (data brokers) do the same. We've identified an indication for increased adoption of Chinese AI companies among Russian-based threat actors, as 12% of Lolz traffic comes from users who visited those services on the same day.

Furthermore, a technical analysis of the threat actor infrastructure reveals a pervasive trend of "vibe coding," the term used when AI assists in the rapid generation of professional-looking SaaS platforms, such as paste sites and virtual number services, without understanding the underlying logic. This AI adoption trend allows actors to scale operations and outsource marketing operations, including the creation of landing pages, to free up more time for hacking.

The Evolution of the Threat Actor

The modern threat actor has evolved from a specialized hacker into a diversified B2B service provider. Case studies of prominent actors, such as JuliusCaesar, demonstrate a shift toward operating legitimate-looking ecosystems—including crypto exchanges and subscription-based OSINT tools—alongside illicit trade. In this zero-trust environment, the primary currency is a form of "community credit," where successful actors distribute free tools and knowledge to establish the authority necessary to monetize their specialized services.

Architectures of Displacement

The 2026 cybercrime landscape is characterized by a fluid form of resilience. Despite frequent law enforcement interventions, the underground economy continues to adapt. Understanding modern threat actor operations requires examining the structural shifts that drove this evolution.

The current threat environment is the product of a cyclical pattern of displacement and reorganization driven by two opposing historical forces over the past three years.

Law Enforcement Disruptions of Traditional Forums

For years, centralized deep- and dark-web forums functioned as the primary hubs for recruitment and illicit trade. However, escalating international law enforcement operations have compromised these environments, fundamentally eroding trust in centralized web infrastructure.

Beginning in 2023, major hubs were systematically dismantled. The repeated seizures of BreachForums—first by the FBI in June 2023, again in May 2024, and culminating in a definitive multinational operation in August 2025 that turned its infrastructure into a law enforcement honeypot—demonstrated the vulnerability of forum administrators whom authorities chose as the main targets. Furthermore, the January 2025 dismantlement of Cracked[.]io during Europol's Operation Talent severed critical arteries for credential stuffing and the distribution of hacking tools.

Fear of infiltration and imminent domain seizure drove a large exodus to mainstream platforms such as Telegram and Discord.

Shift in Telegram's Operational Security

Until late 2024, Telegram served as the preferred operational alternative for application threat actors. Its robust encryption and lax moderation provided an ecosystem for coordination and real-time commerce, offering the utility of a dark-web forum with the accessibility of a modern social app.

This dynamic shifted abruptly on August 24, 2024, following the arrest of Telegram CEO Pavel Durov in France on charges related to the platform's complicity in facilitating criminal activity. The structural impact of this event materialized a month later.

On September 23, 2024, Telegram radically revised its terms of service. The platform explicitly stated it would provide IP addresses and phone numbers to relevant authorities in response to valid legal requests concerning general criminal investigations. This ended the platform's era of impunity. Realizing their operational security was compromised, threat actors initiated a reverse migration, fleeing Telegram to establish newly cloned deep-web forums, decentralized protocols and fragmented communities.

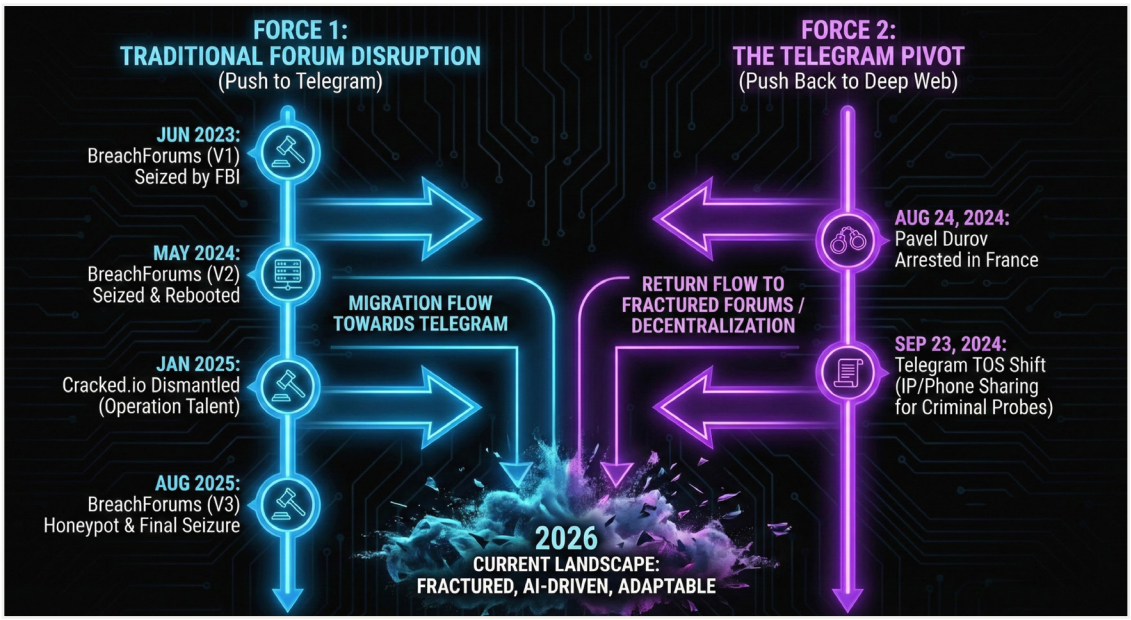


Figure 2:

The evolution of the threat actors' platform migration

2026 Threat Intelligence

Forum Traffic

Analysis of traffic patterns to Cracked, Lolz and BreachForums includes the following measurements:

1. **Total monthly visits** in each forum (January 2026 compared to November 2025) to measure platform popularity

2. **Traffic sources (channels)** to learn about the type of users and how the platform gains its user base

3. **Estimated user age distribution** to learn about the threat actors' years of experience and profile

4. **User cross-visit percentage with AI services** to discover the percentage of users who visited AI services on the same day they visited the forum, revealing the user's favorite AI tools and determining their usage type

Each of these forums focuses on a different hacking type, experience level and audience location:

- **Cracked** targets a U.S.- and global-based audience and focuses on account cracking using automated bots and scripts

- **Lolz** targets a Russian-based audience and focuses on account cracking using infostealers and social engineering

- **Breached** targets a global audience and focuses on leaked/breached database trading

Marketplace Analysis

We've run each of the three target forums through SimilarWeb, a powerful web analysis tool often used in marketing and search engine optimization (SEO). This is an estimation engine, not an exact measurement tool. It relies on four primary sources:

1. A network of millions of users sharing anonymized clickstream data via browser extensions
2. ISP/DSP partnerships that provide broad traffic volume and location logs
3. Direct measurements from site owners who connect their analytics
4. Crawling of map site structures

SimilarWeb essentially uses direct data to train its algorithms. It then applies those learnings to the network and ISP samples to correlate global traffic, engagement and audience demographics for almost every site on the internet.

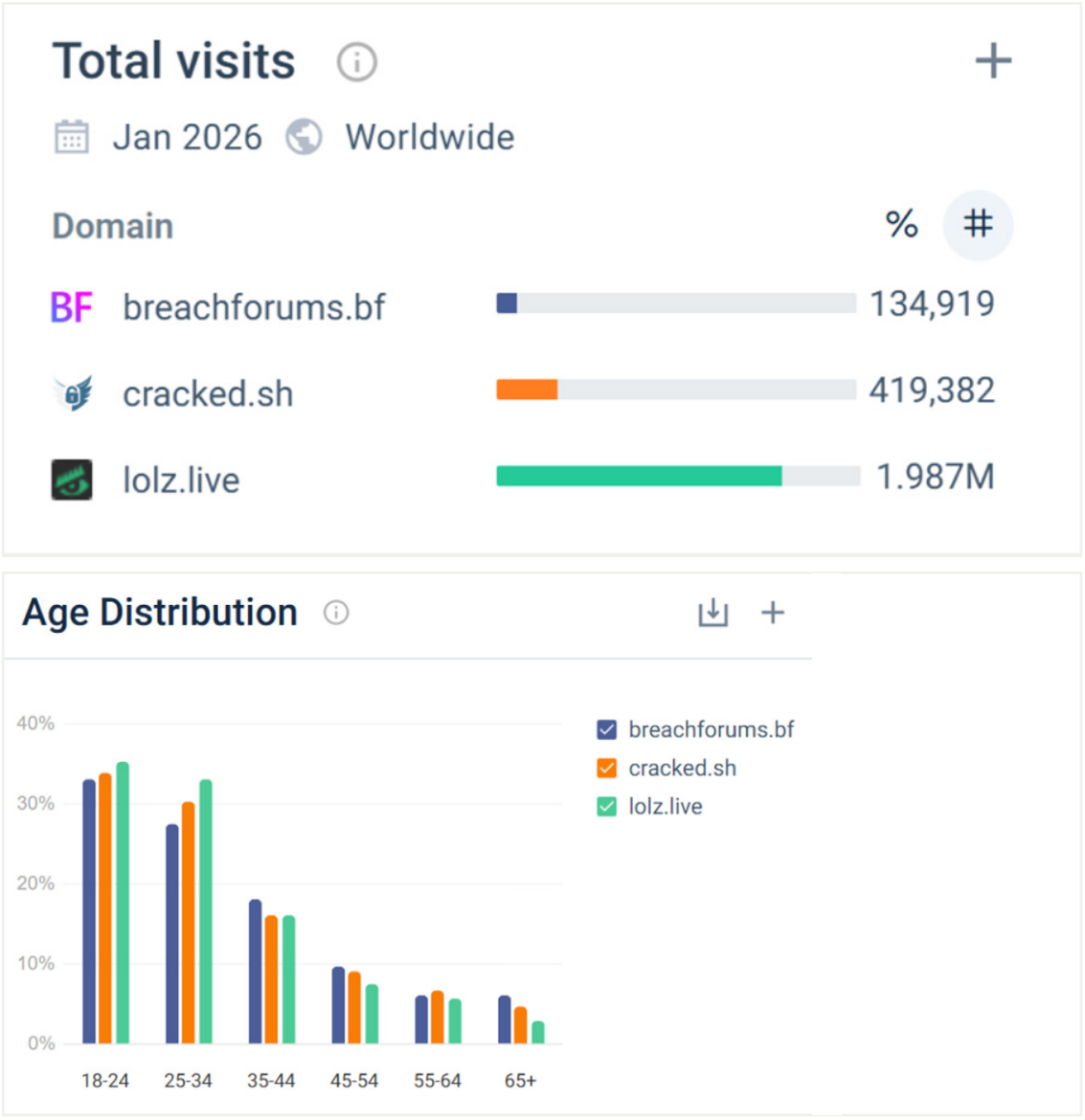


Figure 3:

Monthly traffic by forum in January 2026 (top), age distribution by forum (bottom) (source: Similarweb)

Overall Findings

1. These forums had a total of 2.5 million entries during January 2026

2. Traffic distribution discoveries:

    - **Lolz:** This forum focuses on gaming and infostealers, targeting a Russian-speaking userbase. It leads with almost 2 million monthly visits. As an entry-level forum that serves many gamers who collect cheats and breached gaming accounts, it makes sense.

    - **Cracked:** This dedicated cracking forum targeting U.S. users. It receives 419,000 monthly visits, a relatively high number for a seized forum from the deep web.

    - **BreachForums:** This dedicated forum for breached data brokers and spammers has a global audience that delivers 135,000 monthly visits.

3. Age distribution: In our 2024 research report, "The Hacker Persona," we identified that many new advanced application threat actors were 16 years old and highly engaged in gaming. This pattern appears be holding, with one out of three visits coming from people 18 to 24 years old.

One of the main reasons we see these numbers within the young threat-actor segment is that these forums have become more popular since Telegram strengthened its privacy policy following Alex Duruv's arrest. Threat actors selling cracking services migrated back to deep- and dark-web forums, and their followers (potential buyers) went with them.

How Sites Most Targeted by Law Enforcement Maintained Popularity

We selected our research subjects from twelve well-known threat-actor forums based on their traffic and unique user rates. As a result, these forums receive more exposure from potential threat actors than any other forums we've researched.

Although each of our research targets differs from the others, all three share one thing in common: They were previously shut down or blocked by authorities and later returned under a new URL.

- Breached Forums was seized by the authorities in March 2023, May 2024 and Oct 2025.

- Cracked[.]sh was seized by the authorities in January 2025 (Operation Talent).

- Lolz[.]live was never seized by the authorities. It did, however, quietly migrate from Lolz[.]guru to Lolz[.]live between late 2023 and early 2024. The motivation for the move was Roskomnadzor, the Russian federal executive body responsible for regulating, monitoring, and censoring all media, telecommunications, and information technology. Roskomnadzor intensified its blocking of VPNs and information-stealing marketplaces.

How the Forums Regained Popularity

Let's examine their lead traffic sources:

Figure 4:

Monthly forum traffic per traffic source in Jan 2026 (source: Similarweb)

Direct

Domain	Total traffic
breachforums.bf	66.37%
cracked.sh	77.17%
lolz.live	43.53%

Organic Search

Domain	Total traffic
breachforums.bf	24.29%
cracked.sh	15.69%
lolz.live	40.70%

1. **Cracked:** "The Fortress" (Insular and vetted, the most "closed" community of the three)

↗ **Data:** 77% direct, 15% organic

↗ **Interpretation:**

- Almost four out of five users type the URL directly or use a bookmark. They aren't just "finding" Cracked, they already live there.
- Low organic traffic results indicate that they have poor SEO visibility or actively block search crawlers (OpSec conscious).
- This traffic pattern signals a high-retention, highly skilled user base, where the "quiet professionals" are found.

2. **Lolz:** “The Supermarket” (Commercial and noisy)

↗ **Data:** 43% direct, 40% organic, 14% referrals

↗ **Interpretation:**

- This type of traffic barely fits the typical deep forum statistics that we usually observe; it more closely resembles the traffic patterns of a standard e-commerce website.
- The massive 40% organic traffic result is an indicator that search engines publicly index their threads, marketplaces or profiles.
- High referral rates confirm surface-web blogs, YouTube videos and Telegram channels are linking to them.
- They trade OpSec for volume. They want new members, including skids, buyers and tourists, to find them via search queries like “cheap steam accounts” or “config files.”

3. **BreachForums:** “The Brand” (Notorious and targeted, this profile fits a “famous” illicit site)

↗ **Data:** 66% direct, 24% organic.

↗ **Interpretation:**

- High rates of direct traffic show a strong core of regulars (the actual leakers and brokers).
- Moderate organic traffic is considered an “infamy tax.” This traffic doesn’t reflect people stumbling upon it; it reveals people searching for the brand name (“BreachForums URL” or “latest breach leak”) after seeing it in the news.
- It has the core user base of Cracked, but the public attention of Lolz. This is where the major leaks are published to get maximum media attention.

Overall, the direct traffic percentage for the formerly seized forums, Breached and Cracked, is 72%.

Breach forums, which were seized three times and received extensive media coverage, account for 24% of organic search traffic. This means that one out of four visitors searches for “breach forum” or a related term and, after a few clicks, finds the forum.

A possible scenario:

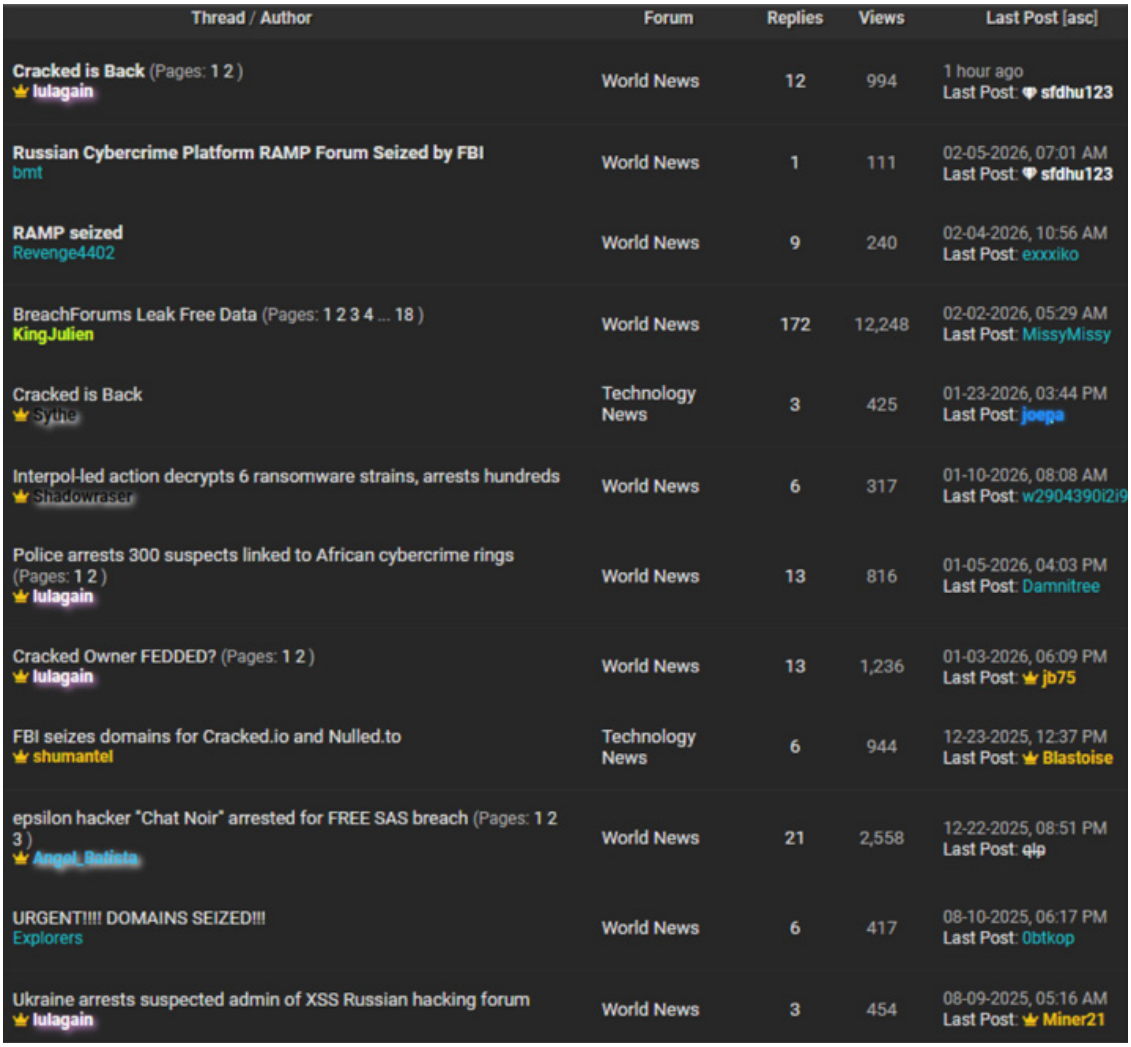
1. Each forum has a “cybernews” section. Below are examples of new posts reporting newly seized forums.

2. The media report follows with a wave of coverage that includes the forum’s name.

3. Potential and curious threat actors search the name through internet search engines/Telegram/Discord. Eventually, they figure out the new forum’s domain name.

Figure 5:

New posts reporting recently seized forums (source: breachforums.as)

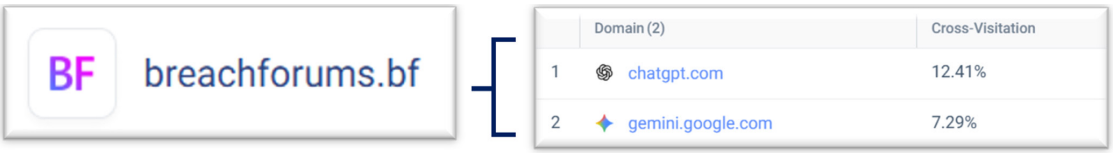


Thread / Author	Forum	Replies	Views	Last Post [asc]
Cracked is Back (Pages: 1 2) lulagain	World News	12	994	1 hour ago Last Post: sfdhu123
Russian Cybercrime Platform RAMP Forum Seized by FBI bmt	World News	1	111	02-05-2026, 07:01 AM Last Post: sfdhu123
RAMP seized Revenge4402	World News	9	240	02-04-2026, 10:56 AM Last Post: exxxiko
BreachForums Leak Free Data (Pages: 1 2 3 4 ... 18) KingJulien	World News	172	12,248	02-02-2026, 05:29 AM Last Post: MissyMissy
Cracked is Back Sythe	Technology News	3	425	01-23-2026, 03:44 PM Last Post: joega
Interpol-led action decrypts 6 ransomware strains, arrests hundreds Shadowraser	World News	6	317	01-10-2026, 08:08 AM Last Post: w2904390i2j9
Police arrests 300 suspects linked to African cybercrime rings (Pages: 1 2) lulagain	World News	13	816	01-05-2026, 04:03 PM Last Post: Damnitree
Cracked Owner FEDDED? (Pages: 1 2) lulagain	World News	13	1,236	01-03-2026, 06:09 PM Last Post: jb75
FBI seizes domains for Cracked.io and Nulled.to shumantel	Technology News	6	944	12-23-2025, 12:37 PM Last Post: Blastoise
epsilon hacker "Chat Noir" arrested for FREE SAS breach (Pages: 1 2 3) Angel_Batista	World News	21	2,558	12-22-2025, 08:51 PM Last Post: qip
URGENT!!!! DOMAINS SEIZED!!! Explorers	World News	6	417	08-10-2025, 06:17 PM Last Post: 0btkop
Ukraine arrests suspected admin of XSS Russian hacking forum lulagain	World News	3	454	08-09-2025, 05:16 AM Last Post: Miner21

BreachForums: The "Old School" Broker

Figure 6:

BreachForums[.]bf cross-visit rate with AI services in Jan 2026 (source: Similarweb)



Signal: Lowest AI usage (only ~12% ChatGPT).

- The relatively low AI usage combined with the presence of Gemini suggests standard web users, likely U.S.-based, who treat AI as a search engine rather than a coding companion.
- **Attack type:** Human-INT, data trading
  - The lack of AI overlaps tells you their work is manual. They are downloading SQL dumps, negotiating ransom prices or leaking documents. You don't need ChatGPT to sell a database.
- **Persona:**
  - They are there to do business, not to learn how to code. The low reliance on technology makes them, ironically, more dangerous, as they deal with raw intelligence rather than script-kiddie tools.

Cracked: The "AI-Augmented" Developer

Figure 7:

Cracked[.]sh cross-visit rate with AI services in Jan 2026 (source: Similarweb)

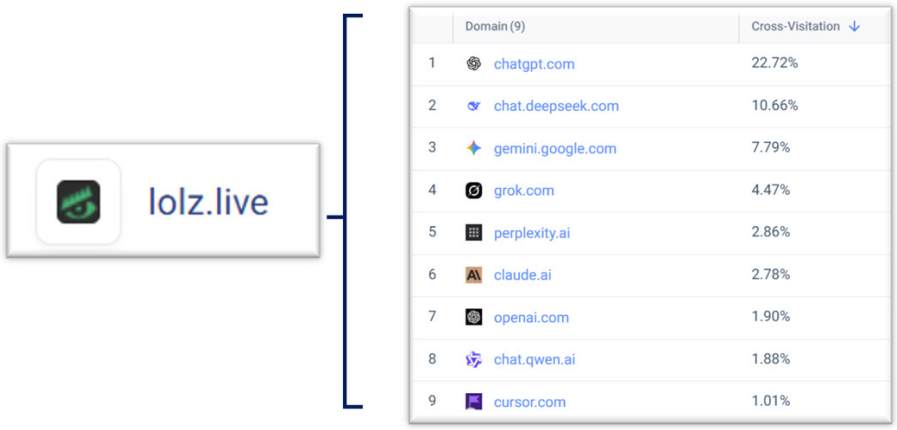
Signal: A massive 47.77% overlap with ChatGPT and significant Claude usage. Almost two-thirds of the user base is actively using an LLM while browsing.

- **Attack type:** Malware development and tool creation
  - Why? You don't need AI to read a forum. You need AI to write code. This confirms Cracked is primarily a technical workshop. They are likely using ChatGPT to write Python scripts for scraping, bypassing WAFs or creating config files for cracking tools.
- **Persona:** "The lazy developer"
  - They are competent enough to run tools but rely on AI to write the code. They are efficiently weaponizing LLMs.

Lolz: The “Eastern Bloc” & “Budget” Threat

Figure 8:

Lolz[.]live cross-visit rate with AI services in Jan 2026 (source: Similarweb)



Signal: The presence of DeepSeek (10.66%) and Qwen (1.88%).

- **Attack type:** High-volume automation (spam/phishing)
  - The mix of tools suggests script kiddies and low-tier developers. They are likely using these AIs to generate phishing templates in multiple languages to debug simple “checker” scripts for account takeovers.
- **Persona:**
  - They aren’t sophisticated hackers; they are volume-based cybercriminals looking for cheap or free tools to scale their operations.

Findings and Insights

1. **Migration rather than a cessation of activity**

    - **Finding:** Despite repeated law enforcement interventions, the three target forums (Cracked, Lolz, and BreachForums) generated 2.5 million visits in January 2026, with a significant demographic concentration of one in three visitors in the 18 to 24 age range.

    - **Insights:** The cybercrime ecosystem exhibits fluid resilience and law enforcement disruptions often increase awareness, driving them to search for the new URLs of the seized forums.

2. **Favorite AI tools**

    - **Finding:** Cross-visit analysis indicates that 47.77% of Cracked users visited ChatGPT on the same day, whereas only ~12% of BreachForums users engage with AI services.

    - **Insight:** AI adoption is not uniform across the underground but is role and GEO-dependent. It has become an essential force, a credential stuffing threat actor, while remaining less relevant to data brokers.

3. **Chinese AI adoption among Russian users**

    - **Finding:** 10.66% of the Russia-based forum Lolz visited DeepSeek chat on the same day of visiting the forum and 2% visited Quen.ai. Both are China-based AI companies.

    - **Insight:** Two options: Either China-based threat actors visit this Russia-based forum, or the Russia-based users are adopting Chinese AI technologies. We believe it's the second option, since although Russian users can access Western AI services, paying the subscription can be challenging due to restrictions on Russian payment providers.

2026 Threat Intelligence

Threat Actor Case Studies

Each forum allows signed-in users to view every user profile, including all of its threads, posts, credits and awards. In this chapter, we will examine two specific threat actor profiles to understand their focus, business model and online presence.

Paste sites dominate deep web forums because they provide a secure, high-capacity layer for sharing sensitive data that forums cannot handle. They offer superior OpSec through client-side encryption and “burn-after-read” settings that leave no digital trail. Furthermore, they act as a resilient fail-safe, ensuring that stolen data or proof-of-concept samples remain accessible even if the primary forum is taken down by law enforcement.

What is a paste site, and why is it in every threat actor’s bookmark bar?

JuliusCaesar: Account Cracker

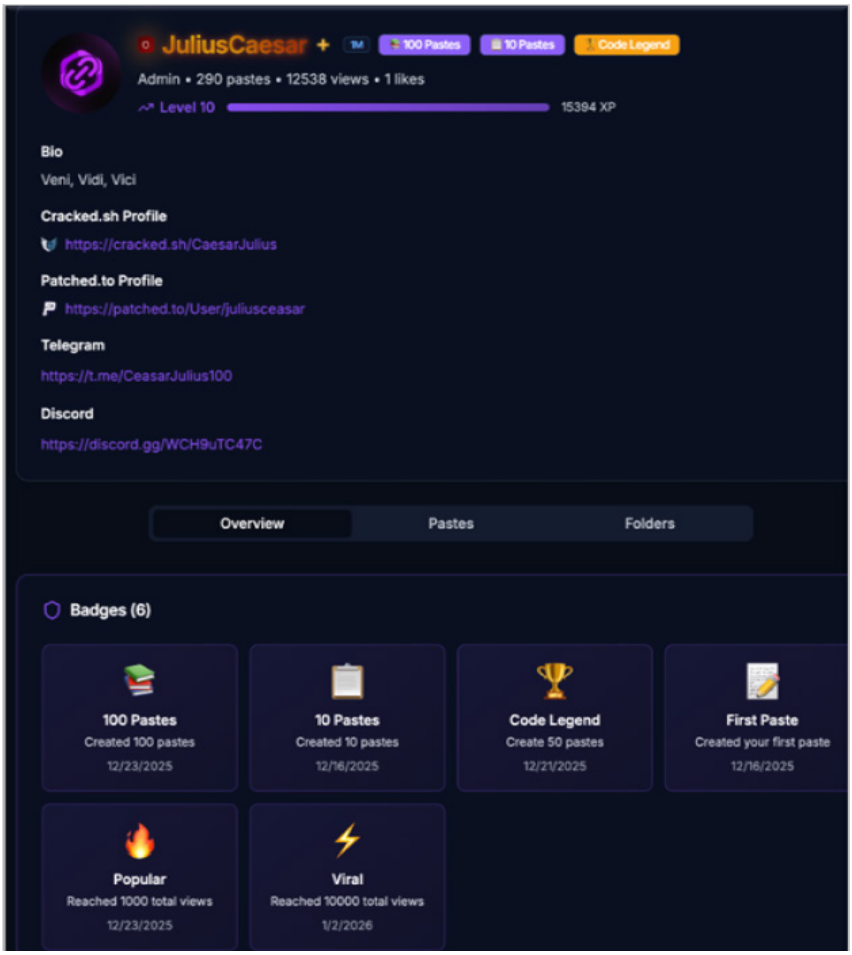
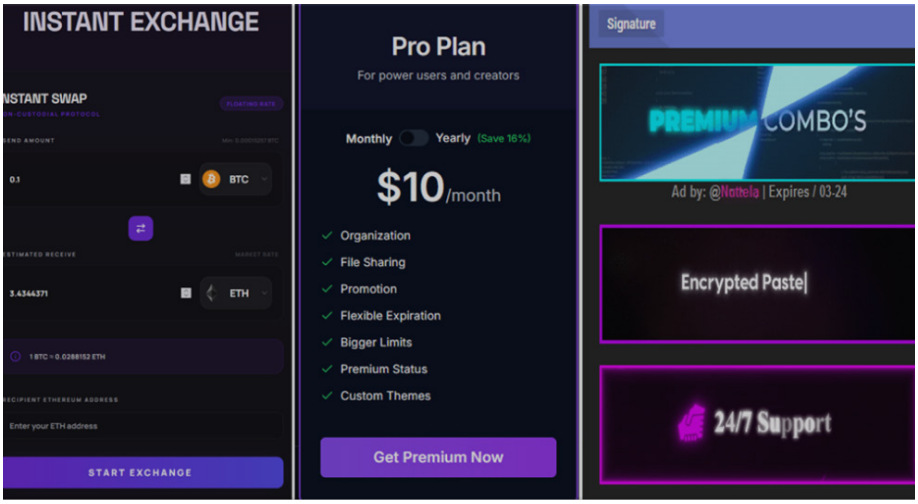


Figure 9:

JuliusCaesar profile on its own paste site

Figure 10:

Juli (left), Coinux.su (center), Mysnippet.dev pro plan (right) (source: Similarweb)



Threat actor's type: Account cracker

Attack type: Credential stuffing using bots

Business: JuliusCaesar has two businesses:

1. **Mysnippet.dev** – A paste site built with AI featuring ads and a pro plan subscription (Figure 10, right)
2. **COINUX.SU** – A crypto exchange platform gaining transaction fees from exchanging its users' cryptocurrency (Figure 10, center)

JuliusCaeser also offers a placeholder in its profile signature, turning it into an advertising billboard (Figure 10, left)

Strategy:

1. Cracks accounts from all industries, selling them on different platforms and sharing 10-15% of them for free using his own paste site
2. Publishes a thread across forums that lures viewers into his own paste site
3. Monetizes ads on his profile through his signature and on his paste site

Katz: Config Developer

Active since: Oct 2, 2018

Threat Actors type: Config Developer – API Attacker

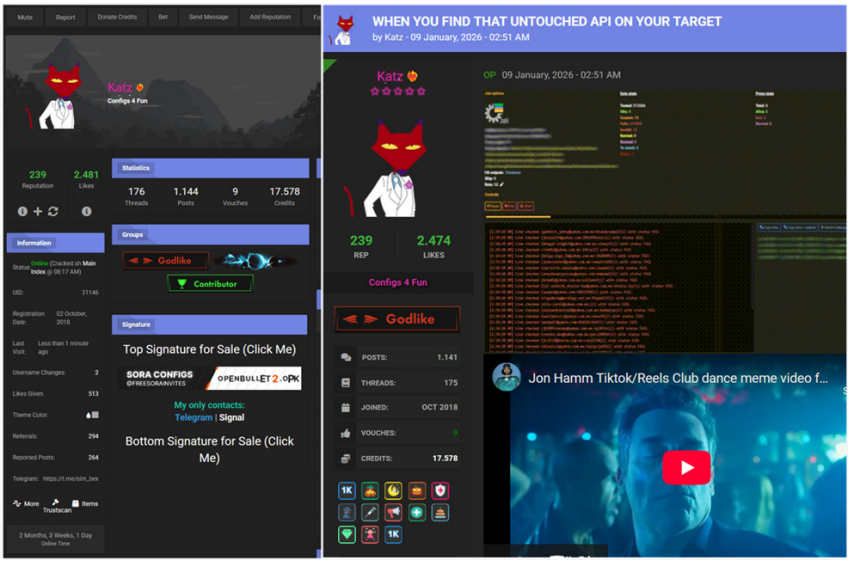
Attack type: Credential stuffing using bots

Strategy and business module: Katz has two businesses:

1. Constantly shares cracking tools, tutorials and configs for free to increase credit score and credibility
2. Sells credential stuffing attack script in crypto. On top of this, it sells a placeholder in his profile signature that turns it into an advertising billboard (Figure 11, left)

Figure 11:

Katz's profile page (left) is an example of a thread.



Findings and Insights

1. Multi-business, multiple faces

- **Finding:** Profiles of prominent actors like JuliusCaesar reveal a shift toward diversified service models, where actors operate legitimate-looking SaaS platforms, such as paste sites and crypto exchanges, alongside traditional illicit activities.

- **Insights:** The modern advanced threat actor is evolving from a specialized hacker into a diversified service provider, building resilience by creating an ecosystem of revenue streams that mimics legitimate B2B structures.

2. Community credit value

- **Finding:** Successful actors like Katz distribute significant amounts of free tools, configurations and tutorials before attempting to monetize specific high-value scripts.

- **Insight:** In a zero-trust environment, community credit remains the primary currency; establishing technical authority through knowledge transfer is a necessary precursor to financial success in the underground economy.

One of the most frequently observed and cross-platform findings in our research was a significant increase in new SaaS businesses focused on hacking. It seems that almost every active threat actor now has either a shop, a website or a site for SaaS hacking services. Was it vibe coded? We analyzed the HTML files of 12 hacking websites in search of smoking gun evidence. This is what we looked for:

Identifying AI-Generated "Vibe" Code

The logic behind identifying AI-written code centers on one key truth: humans prioritize long-term maintenance and logical structure, while AI focuses on immediate visual output (the "vibe") in a single instance. When searching for signs of AI involvement, it's important to shift focus from design elements to decision-making processes. This is why we created a definitive framework for uncovering AI-generated code based on our analysis:

1. Platform-specific Functions in AI App Builder Services

Some vibe coding platforms that offer instant website generation leave a clear trail in the site's HTML. See the Snippet.dev analysis below.

2. The Single-File Obsession (Lack of Modularity)

Humans dislike cluttered workspaces, opting for external style sheets (.css files) and linking to icon libraries to keep the main HTML file clean and readable. In contrast, AI typically delivers self-contained products unless specifically instructed otherwise.

- **Possible indicators:** Look for large blocks of inline CSS embedded in the '<body>', repeated raw SVG mathematical strings instead of leveraged icon libraries or extensive JSON configurations (like the '__next_f' blob) hardcoded at the page's end.

3. Extremes of Complexity (Archaic vs. Over-Engineered)

AI lacks the human intuition of choosing the right tool for the job. It often swings between two extremes based on its prompts.

- **Possible Indicators:** It either relies on deprecated, ancient tags (like) because they are mathematically easy to output for simple layouts, or it defaults to heavy, enterprise-grade frameworks (like Next.js) to build a static landing page because that framework dominates its training data. There is rarely a sensible, lightweight middle ground.

4. Overlapping Code Blocks

Human developers typically look for efficiency; we use loops for repetitive tasks and CSS rules for complex designs. AI, being tireless, does not concern itself with file size or the number of keystrokes.

- **Possible Indicators:** Evidence can be seen in the hardcoding of 25 identical, overlapping tags to achieve a 3D visual effect or repetitively copy-pasting the same testimonial HTML block multiple times instead of applying a concise array loop.

5. Contextual Amnesia and Token Glitches

AI models process text sequentially and often lose the plot on longer generations due to the token limit.

- **Possible Indicators:** This can lead to confusing logic, such as defining a CSS animation in the <head> tag of an HTML document and then writing a JavaScript function to inject the same animation again at the bottom of the page. An even more problematic scenario occurs when the token limit is reached, leaving critical syntax errors (like 'this.src='https:') unaddressed in live production code.

Below are three examples of threat actor websites that strongly indicate the use of AI in their creation.

Snippet.dev (Encrypted Paste Sharing)

This analysis of **Snippet.dev** reveals a professional-level, AI-generated signature that's a step above the messy vibe-coding seen in the previous example. While the site appears modern and high-quality, the underlying HTML contains undeniable markers of an automated, AI-driven development environment, specifically one using **Vite, React and an AI engineering agent**.

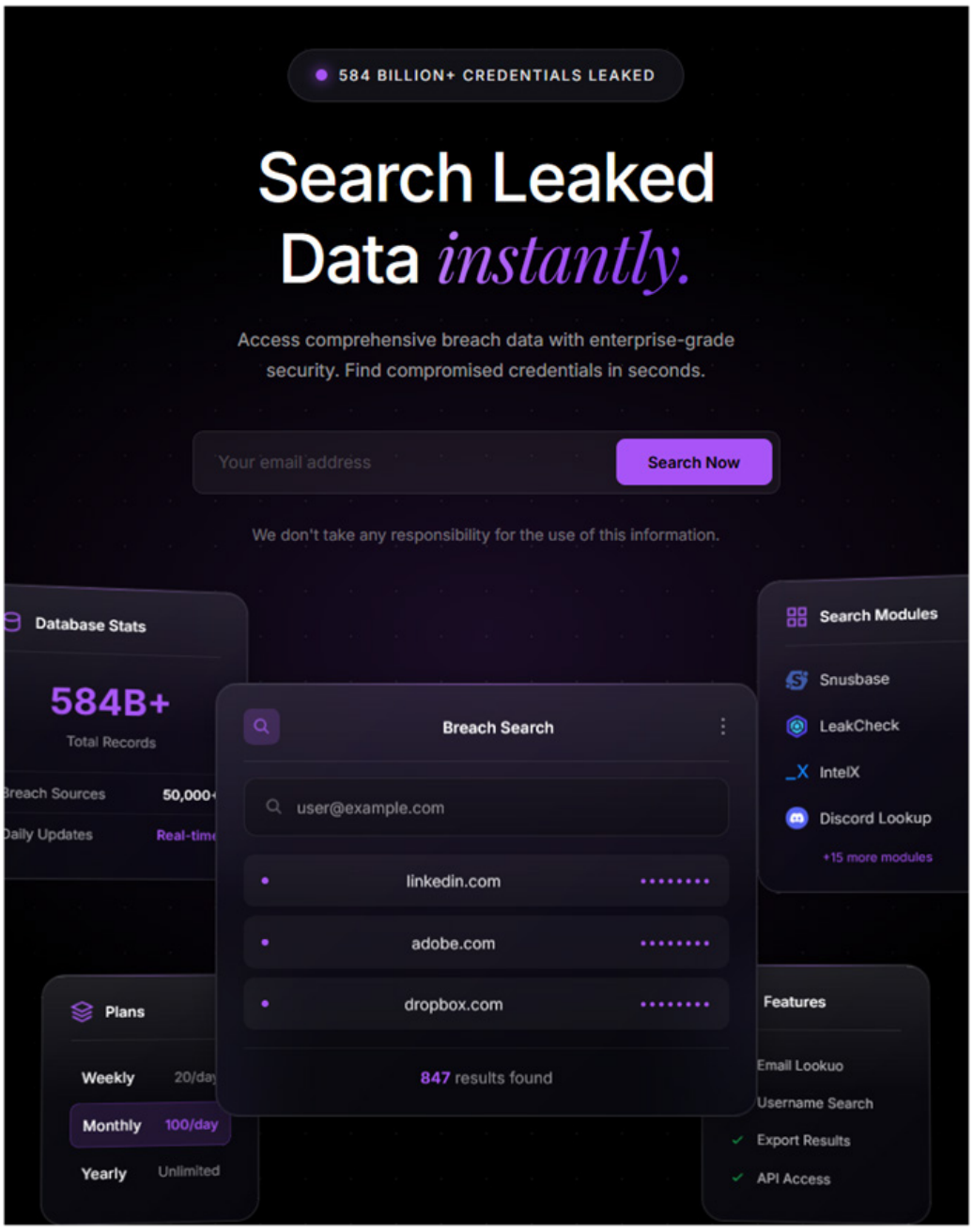
Marker	Evidence in Snippet.dev	Indicatation of AI/Automation
The "Blink" Footprint	<script src="https://blink.new/auto-engineer.js?projectId=animated-paste-site-fm49henh" ...>	**Hard Evidence**. This script links directly to **Blink.new**, an AI-powered "auto-engineer" platform. The project ID "animated-paste-site" is a default-style name generated by AI platforms.
Asset Hashing	/assets/index-BvueZpx7.js, vendor-ui-B47b0Ran.js	These are typical **Vite/Rollup** build artifacts. While common in modern dev, AI tools like **Lovable, Bolt, new**, or **V0 (Blink.new in this case)** use these stacks exclusively because they are highly predictable for LLMs.
Badge-Hiding Logic	A complex script at the top, specifically designed to hide #blink-badge-container	This is a "clean-up" script. The user prompted the AI to build the site, but then had to write (or prompt) a second script to **hide the "Made with Blink" watermark** that appears on free-tier AI projects.
Generic SEO Bloat	Extensive Open Graph and Twitter meta tags with perfect, repetitive descriptions	AI tools generate exhaustive SEO metadata by default to give the "vibe" a professional feel, even if the site is a temporary "burner".

- Blink (Blink.new): An AI-powered auto-engineer platform that builds complete, full-stack web applications—including the backend infrastructure and databases—from a single natural language prompt.
- Vite / Rollup: Vite is a modern, high-performance frontend build tool, while Rollup is the underlying module bundler it uses to compile, optimize and bundle code for production.
- Lovable: A full-stack AI development platform that generates fully functioning, editable web applications with real source code based entirely on text prompts.
- Bolt.new: An AI web development agent powered by StackBlitz that allows users to prompt, run, edit and deploy full-stack browser-based applications without needing a local dev environment.
- v0 **(by Vercel)**: An agentic AI tool that generates, builds and deploys production-ready user interfaces and full web applications directly from plain English descriptions.

Stolen.tax (Breached Credentials as a Service + Intelligence Tool)

Figure 12:

Stolen.tax website - breached data as a service (source: Stolen.Tax)



Indicator	Technical Reality	Indication of AI
The "Token Limit" Glitch	The code contains an unclosed, fatal syntax error: <img ... onerror=" this.src='https: followed immediately by .	AI generators can hit token limits or encounter "glitch tokens" that abruptly truncate code strings mid-generation. A human developer's code editor would instantly highlight this massive error in red; the operator here copied and pasted the raw, broken output.
Schizophrenic CSS Logic	The identical @keyframes spin animation is defined once in the <head> and injected a second time via a JavaScript function at the absolute bottom of the file.	LLMs frequently lose track of context over long generations. It forgot it already wrote the CSS and generated a Redundant JS function to do it again. Humans do not write identical logic in two completely different languages in the same file.
Hardcoded Raw SVGs in JS	The executePublicSearch function injects a massive, unreadable raw SVG string directly into btn. innerHTML to create a loading spinner.	AI optimizes for self-contained, single-file solutions. A human developer would toggle a clean CSS class (e.g., btn.classList. add('loading')) or reference a stored asset rather than dumping raw vector math into a script.
Inconsistent Fallbacks	The image onerror attributes use completely different, disconnected external URLs (like Iconify and IOC Exchange) as fallbacks if the primary image fails to load.	The AI hallucinated or scraped various disconnected external URLs from its training data. A human standardizes error handling (e.g., pointing all broken images to a single local file, such as/assets/ default-icon.png).
Critical DOM-Based XSS	The application takes raw JSON API responses (item.email) and renders them directly into the browser using .innerHTML without sanitization.	AI understands the visual requirement ("display search results") but frequently lacks contextual awareness of the threat model. Passing untrusted data directly to DOM sinks, such as innerHTML, creates a fatal security hole. It builds the feature but leaves the door wide open.

The person operating this platform does not have the technical depth to build their own frontend. They rely entirely on AI to create a slick, convincing, "pink-themed" cyberpunk veneer to sell subscriptions.

Does this mean their database is fake? Not necessarily. They might have aggregated 584B+ credentials (or more likely, bought/downloaded public collections like COMB and hosted them). But their operational security and development skills are sloppy. If they are this lazy on the frontend—leaving literal broken strings of code on their live landing page—their backend API and security implementations are almost certainly just as hastily patched together.

Sms.sb (Virtual Phone Number Provider)

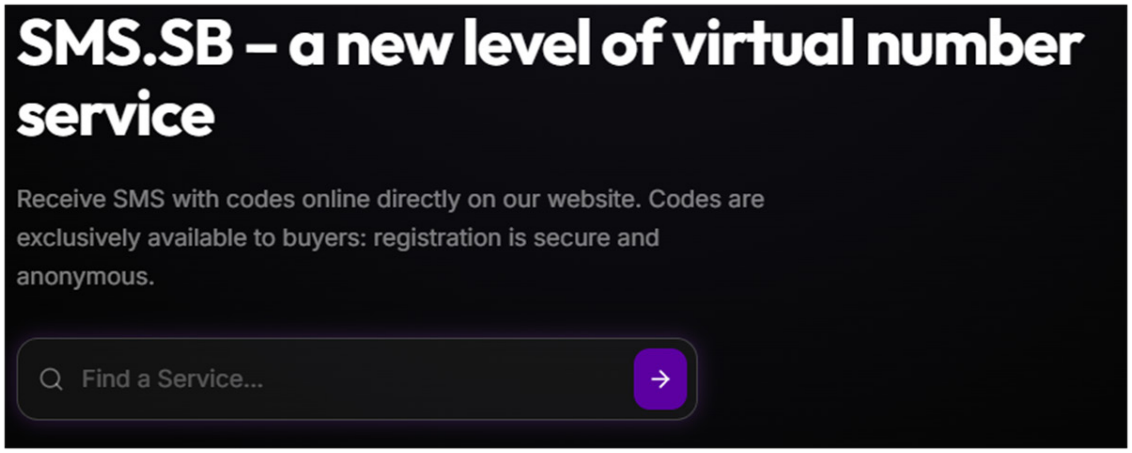
This platform that allows anyone with a crypto wallet to receive SMS with a temporary virtual phone number.

User type:

1. Application threat actors that engage in fake account creation/account farming, since most of the applications require phone number verification when signing up
2. Account crackers that want to lock the victim outside of their account by turning on 2FA with a virtual phone number
3. Spammers/Social engineers to launch a phishing campaign

Figure 13:

Sms.sb services search (source: Sms.sb)



Smoking Gun Indicators

Indicator	Technical Reality	Indicators of AI
The "Next.js + Tailwind" Stack	The HTML is full of classes like min-h-screen, overflow-x-hidden, relative, and _next/static paths.	This is the "default" output for modern AI web generators (v0, Bolt). They almost exclusively use this stack because the documentation is massive and the AI handles it perfectly.
Lucide Icon Overload	Every single icon (sparkles, search, zap, lock) is a perfectly injected SVG with standardized Lucid classes.	While humans use Lucide, AI generators inject the entire SVG code directly into the HTML to ensure the "vibe" is captured in a single preview, rather than linking to an external library.
The "Next.js __next_f" JSON Blob	At the bottom of the file (lines **250+**), there is a massive block of serialized JSON data.	This is a byproduct of **Next.js App Router**. While humans use Next.js, AI builders generate these complex, high-performance frameworks by default because they provide the most "impressive" initial result.

Findings and Insights

1. **Vibe Coding trend among threat actors**

    - **Finding:** Eight out of 12 analyzed threat actor websites show distinctive indicators of AI use. These indicators, include unoptimized single-file structures, artifacts from auto-engineering tools like Blink.new, and fatal syntax errors caused by LLM token limits.
    - **Insight:** There is a growing trend of “vibe coding” among threat actors who prioritize the speed and visual aesthetic of their infrastructure over logical stability, often relying on AI to build platforms where they lack the technical depth to manually debug.

2. **What are they building**

    - **Finding:** The three most frequently observed sites: paste sites, database-as-a-service sites and virtual phone services.
    - **Insight:** It seems that AI-written code fuels the underground economy as almost every threat actor with access to breached information can open a SaaS business to target the cracking community.

Forum Traffic

1. **Migration rather than a termination of activity**
    - **Finding:** Despite repeated law enforcement interventions, the three target forums (Cracked, Lolz, and BreachForums) generated 2.5 million visits in January 2026, with a significant demographic concentration of one in three visitors in the 18 to 24 age range.
    - **Insights:** The cybercrime ecosystem exhibits “fluid resilience” and law enforcement disruptions often increase awareness, driving searches for the new URLs of the seized forums.

2. **Favorite AI tools:**
    - **Finding:** Cross-visit analysis indicates that 47.77% of Cracked users visited ChatGPT on the same day, whereas only ~12% of BreachForums users engage with AI services.
    - **Insight:** AI adoption is not uniform across the underground but is role and GEO-dependent. It has become an essential force, a credential stuffing threat actor, while remaining less relevant to data brokers.

3. **Chinese AI adoption among Russian forum users:**
    - **Finding:** 10.66% of the Russian-based Lolz[.]live forum visited DeepSeek chat on the same day and 2% also visited Quen.AI. Both are Chinese companies.
    - **Insight:** Either China-based threat actors visit this Russian-based forum, or the Russian-based users are adopting Chinese AI technologies. We believe it’s the second option, since although Russian users can access Western AI services, paying the subscription can be challenging due to restrictions on Russian payment providers.

Threat Actor Case Studies

1. **Multi-business, multiple faces**
    - **Finding:** Profiles of prominent actors like JuliusCaesar reveal a shift toward diversified service models, where actors operate legitimate-looking SaaS platforms (such as paste sites and crypto exchanges) alongside traditional illicit activities.
    - **Insights:** The modern advanced threat actor is evolving from a specialized hacker into a diversified service provider, building resilience by creating an ecosystem of revenue streams that mimics legitimate B2B structures.

2. **Community credit value**
    - **Finding:** Successful actors like Katz distribute significant amounts of free tools, configurations, and tutorials before attempting to monetize specific high-value scripts.
    - **Insight:** In a zero-trust environment, “community credit” remains the primary currency; establishing technical authority through knowledge transfer is a necessary precursor to financial success in the underground economy.

Hacker’s Vibe Coding

1. **Vibe coding trend among threat actors**
    - **Finding:** Eight out of 12 analyzed threat actor websites show distinctive indicators of AI use. These indicators include unoptimized single-file structures, artifacts from auto-engineering tools like Blink.net, and fatal syntax errors caused by LLM token limits.
    - **Insight:** There is a growing trend of “vibe coding” among threat actors who prioritize the speed and visual aesthetic of their infrastructure over logical stability, often relying on AI to build platforms they lack the technical depth to manually debug.

2. **What are they building**
    - **Finding:** Landing pages and websites of their hacking services and products. The three most frequently observed types of sites are paste sites , database-as-a-service sites and virtual phone services.
    - **Insight:** It seems that AI-written code fuels the underground economy, as almost every threat actor with access to breached information can open a SaaS business, targeting the cracking community with AI-generated websites, banners and ads. Outsourcing marketing, sales and support to AI frees a lot of time for application threat actors to redirect to what they are good at: hacking.

2026 Threat Intelligence

List Of Figures

Methodology

1. Forum traffic: We analyzed 12 deep web forums using the SimilarWeb traffic analysis tool and chose BreachForums, Cracked, and Lolz as representatives of both US- and RU-based hacking communities. We focused on application attacks and high traffic compared to other known forums.
2. Threat actor chapter: Using several aged accounts on the target forums, we reviewed 264 threat actor profiles, diving into their threads and posts from their first activity to the most recent.
3. We reviewd the HTML of threat actors' sites and researched indications for AI-written code.

Author

Arik Atar I Senior Cyber Threat Intelligence Researcher

Production

Jeffrey Komanetsky I Senior Content Development Manager

Kimberly Burzynski I Senior Marketing Communication Manager

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

RWI6319 | 03.25.2026