

CYBERCRIMINAL FORUMS

AN IN-DEPTH ANALYSIS OF UNDERGROUND COMMUNITIES, TRENDS, AND THREAT LANDSCAPE

Jeremy Makowski
Cyber Threat Intelligence Expert
(Crime, Warfare and Counter-Terrorism)

July 2026

Disclaimer **3**
Methodology and Confidence Levels **4**
Executive Summary **6**
1. Understanding Cybercriminal Forums **7**
1.1 Role of Forums in the Cybercriminal Ecosystem 7
1.2 Platform Location and Relative Stability 9
1.3 Registration, Access, and Membership 12
1.4 Law-Enforcement Disruption and Forum Reconstitution 16
2. How Cybercriminal Forums Operate **20**
2.1 Administration and Governance 20
2.2 Trust and Reputation 24
2.3 Transactions and Criminal Business Models 24
2.3.1 Forum Owners as Commercial Intermediaries 25
2.3.2 Trust, Escrow, and Transaction Risk 27
2.3.3 Pricing and Analytical Interpretation 28
2.3.4 Movement from Public Listings to Private Transactions 28
2.4 Forum Infrastructure, Security, and Anonymity 29
3. Main Categories of Cybercriminal Forums **32**
3.1 General Forums **33**
3.2 Language and Regional Forums **35**
3.2.1 Russian-Language and Eastern European Forums 36
3.2.2 English-Language Forums 39
3.2.3 Spanish and Portuguese-Language Forums 40
3.2.4 French-Language Forums 41
3.2.5 Arabic and Middle East-Language Forums 42
3.2.6 Chinese-Language Forums 43
3.2.7 Cross-Language Criminal Activity 44
3.3 Network Access, Compromised Accounts, and Data Leaks forums **45**
3.3.1 Initial access as a commercial product 46
3.3.2 Compromised accounts and identity-based access 47
3.3.3 Data leaks as raw material and strategic leverage 48
3.4 Carding, Financial Fraud, and Identity Crime **49**
3.4.1 The fraud supply chain 50
3.4.2 Products sold in carding communities 51
3.4.3 Identity crime beyond payment cards 51
3.4.4 Services and operational knowledge 52
3.4.5 Trust, deception and market instability 52
3.5 Hacking, Malware, and Cyberattack Services **53**
3.5.1 Malware products and service models 54
3.5.2 Malware-as-a-Service and affiliate structures 54

3.5.3 Hacking-for-hire and specialized services 55
3.5.4 Technical claims and product quality 56
3.5.5 Forums as recruitment and coordination environments 57
4. Threat Actors and Criminal Supply Chains 58
4.1 Main Threat Actors in the Criminal Supply Chain 58
4.2 From Access to Monetization 59
4.3 Criminal Relationships and Intelligence Value 60
5. Forum Assessment and Intelligence Collection 61
5.1 Assessing Forums, Vendors, and Listings 61
5.2 Monitoring Methods and Collection Priorities 63
5.3 Researcher Security, Legal, and Ethical Considerations 64
6. Turning Forum Activity into Actionable Intelligence 66
6.1 Strategic, Operational, and Tactical Intelligence 66
6.2 Intelligence Reporting and Escalation 67
7. Investigative Challenges and Emerging Trends 68
7.1 Investigative Limitations 68
7.2 Evolution of the Forum Ecosystem 69
7.3 Emerging Trends 70
Conclusion 72
About the Author 74
References 75

Disclaimer

This report is made freely available for informational, educational, and research purposes. It is intended to support a deeper understanding of the evolving cybercriminal forums ecosystem and does not constitute legal, operational, financial, or security advice.

The report is based primarily on publicly available information. Although every reasonable effort has been made to ensure accuracy, information concerning cybercriminal forums is often incomplete, rapidly changing, difficult to verify, and subject to deliberate deception. The findings and assessments in this report should therefore be understood in light of the stated methodology, intelligence gaps, and confidence levels.

Any reproduction, quotation, adaptation, or distribution of this report, whether in whole or in part, must include appropriate attribution to the author and a clear reference to the original publication.

Commercial use, resale, or incorporation of this report into a commercial product or service is prohibited without the author's prior written consent.

Methodology and Confidence Levels

This report uses Link-Base (link-base[.]ms) as its principal directory for identifying and classifying cybercrime and hacking forums. Link-Base was selected for its broad historical coverage and ongoing tracking of underground platforms. However, its listings were treated as a discovery and classification resource rather than as an authoritative or comprehensive census of the cybercriminal forum ecosystem. The Link-Base data used in this report were collected in July 2026. Forum status, activity, specialization, accessibility, and technical infrastructure were independently assessed and, where possible, corroborated using additional technical, investigative, and open-source information.

The findings were supplemented and cross-referenced with intelligence obtained from public and restricted-access forums, cybercriminal communities, underground marketplaces, messaging platforms, archived discussions, user profiles, and directly observed activity. Additional sources included technical indicators, threat intelligence reports, security advisories, court documents, corporate registries, domain registration records, infrastructure analysis, and other relevant open-source intelligence. The investigation examines forum structure, activity levels, user communities, thematic specializations, operational characteristics, technical infrastructure, accessibility, longevity, and relationships with broader cybercriminal and underground ecosystems. The report distinguishes among the following categories of information:

- Directly observed forum content and activity
- Forum listings, classifications, and status information recorded by Link-Base
- Technical and infrastructure-related findings
- Information corroborated by multiple independent sources
- Historical and behavioral patterns identified through forum monitoring
- Analytical assessments derived from observable indicators and collected intelligence

The following confidence terminology is used throughout the report:

High confidence indicates that an assessment is supported by multiple reliable and independent sources, directly observed forum activity, authoritative technical evidence, official documentation, or a consistent body of corroborated intelligence.

Moderate confidence indicates that an assessment is supported by credible evidence and observable indicators, although certain intelligence gaps, limitations in forum access, or attribution constraints remain.

Low confidence indicates that an assessment is based on a limited amount of available information or on an activity that could not be examined in sufficient depth.

Confidence levels reflect the quality, scope, reliability, and consistency of the available intelligence rather than the potential severity of the assessed activity or threat. They should be reviewed and updated as additional forum activity, technical evidence, or investigative findings become available.

Executive Summary

Cybercriminal forums are not merely online meeting places where offenders exchange messages. They are enabling infrastructures that organize fragmented criminal capabilities into functioning markets. Within these environments, actors can acquire compromised network access, stolen credentials, malware, personal data, technical expertise, laundering services, and operational partners without having to develop every capability internally. Forums therefore reduce the cost, time, and specialist knowledge required to conduct cybercrime.

Their principal value lies in coordination and in creating trust. Cybercrime inherently exposes criminals to fraud: buyers cannot easily verify the authenticity of stolen data, sellers cannot safely identify customers, and neither party can rely on formal contracts or legal enforcement. Forums partially resolve this problem through reputation systems, escrow services, vendor verification, dispute arbitration, membership restrictions, and public feedback. These mechanisms do not eliminate deception, but they enable repeated commercial interactions between actors who may never know one another's true identities.

The forum ecosystem should not be understood as a single, stable underground. It is distributed across traditional web forums, Tor-based services, marketplaces, messaging platforms, private chat groups, and invitation-only communities. Actors frequently use several platforms simultaneously. A public or semi-public forum may be used for advertising and reputation-building, while negotiations, data delivery, and payments take place through encrypted private channels. Consequently, monitoring only one platform rarely provides a complete understanding of an actor or criminal operation.

Specialization has transformed these environments into a cybercriminal supply chain. One actor steals credentials, another sells access to an enterprise network, another deploys malware, and a separate group launders the proceeds. This division of labor improves criminal efficiency and creates opportunities for actors with limited technical ability to purchase sophisticated capabilities as services. Europol's recent assessments describe stolen data as a central commodity connecting fraud, intrusion, extortion, and other forms of organized crime, while ransomware investigations repeatedly demonstrate the role of access brokers and specialized service providers.

For intelligence teams, forum activity can provide several forms of warning. Strategically, it can reveal changes in criminal demand, emerging service models, and shifts in the geographical focus of threat actors. Operationally, it can identify targeting of a sector, technology, or organization. Tactically, it may expose compromised credentials, vulnerable infrastructure, malware indicators, or specific access offers.

However, forum reporting must be treated as unverified human-generated intelligence. Criminal advertising is frequently exaggerated, recycled, fraudulent or deliberately misleading. The analytical objective is therefore not simply to collect forum posts. It is to determine what a platform, actor, or listing reveals about criminal capability, intent, access, and opportunity. High-quality forum intelligence combines persistent observation, source evaluation, infrastructure analysis, identity resolution, cryptocurrency tracing, technical validation, and wider contextual research. The ultimate measure of value is whether the information supports defensible decisions: reducing exposure, investigating a compromise, protecting an individual, disrupting a criminal service, or anticipating an emerging threat.

1. Understanding Cybercriminal Forums

1.1 Role of Forums in the Cybercriminal Ecosystem

Cybercriminal forums serve as coordination layers for actors with different but complementary resources. A technically capable malware developer may lack access to suitable victims. An initial-access broker may control compromised corporate systems but lack the infrastructure, personnel, or relationships required to monetize them. A fraudster possessing stolen identities may still require forged documents, payment accounts, cash-out specialists, or cryptocurrency-laundering services. Forums allow these actors to identify one another, assess potential partners, and combine separate capabilities into a functioning criminal operation.

Their importance should therefore be assessed in terms of market organization and operational enablement, rather than solely on content volume. A relatively small forum may be strategically significant when it attracts highly specialized vendors, experienced operators, or members of established criminal groups. Conversely, a platform with tens of thousands of registered accounts may contain substantial discussion, recycled material, and low-level trading but relatively little sophisticated criminal activity. Membership numbers, post counts, and public visibility are therefore weak indicators when considered without information about vendor quality, transaction frequency, exclusivity, customer feedback, access restrictions, and connections to external criminal networks.

Forums perform five broad ecosystem functions:

- **Discovery:** connecting buyers with vendors, affiliates, technical specialists, brokers, and operational partners.
- **Commercialization:** transforming stolen access, compromised data, and malicious capabilities into products or services that can be advertised, priced, and traded.
- **Reputation building:** allowing actors to demonstrate reliability, accumulate reviews and establish persistent criminal identities.
- **Knowledge transfer:** distributing tutorials, tools, technical guidance, operational experience, and lessons learned.
- **Coordination:** supporting recruitment, partnerships, subcontracting, and the assembly of temporary or long-term criminal teams.

These functions allow forums to reduce some of the organizational friction that would otherwise limit cybercriminal cooperation. Participants do not necessarily need to know one another personally or belong to the same organization. Reputation systems, escrow arrangements, guarantor services, administrator mediation, and transaction histories can provide limited substitutes for conventional commercial trust. Although these mechanisms do not eliminate fraud, they make cooperation between pseudonymous actors more practical and scalable.

A forum may also operate as a form of **criminal institutional memory**. Archived discussions, tutorials, leaked tools, dispute records, and vendor histories preserve knowledge generated by earlier offenders. New participants can learn from previous campaigns, identify commonly used services, and adopt established criminal practices without having to develop every capability independently. This lowers some barriers to entry, although it does not make all participants equally capable. Large numbers of users remain low-skilled consumers, opportunistic fraudsters or observers, while a much smaller group of developers, brokers, administrators, and experienced operators supply the capabilities responsible for the greatest harm.

The ecosystem is also broader than financially motivated hacking. Forum participants may include organized fraud networks, cryptocurrency launderers, corrupt insiders, data brokers, extortion groups, influence actors, hacktivists, and individuals associated with state-aligned activity. The boundaries between these categories are often indistinct. The same compromised infrastructure, credentials, vulnerability information, or malware may support espionage, fraud, ransomware, influence activity, or politically motivated disruption, depending on the actor who acquires it and the objective for which it is used.

The analytical significance of a forum consequently rests on what the platform enables. A forum advertising access to enterprise networks is important not simply because compromised access is being discussed, but also because it may connect an initial intrusion to a ransomware affiliate, a data-theft group, a fraud network, or an espionage actor. The forum becomes a transfer point where one phase of malicious activity is handed off to another specialist. It may therefore link actors who would otherwise remain separated across different stages of the cybercriminal supply chain.

1.2 Platform Location and Relative Stability

Cybercriminal forums operate across the clear web, the broader deep web, and anonymity networks commonly associated with the dark web. These environments should not be treated as direct indicators of criminal sophistication. A forum's location is generally determined by its operational requirements, intended audience, security model, accessibility needs, and tolerance for public visibility rather than by the seriousness of the activity taking place within it.

In practice, forums operating through conventional internet domains may be more stable and consistently accessible than platforms that rely exclusively on Tor or other anonymity networks. This is particularly true of restricted or invitation-only communities that are technically reachable through the clear web but whose content is protected by registration, vetting, payment barriers, or private access controls. Such platforms form part of the non-indexed deep web even though their infrastructure is not necessarily hidden.

Clear- and deep-web forums can benefit from mature commercial hosting, content-delivery networks, anti-DDoS protection, domain redundancy, and easier access for users. They can also integrate more readily with encrypted messaging applications, cryptocurrency services, external marketplaces, and public announcement channels. Established forums may change domains, hosting providers or registrars while preserving their databases, branding, membership structures, and reputation systems. From the user's perspective, these mechanisms can provide greater continuity than is commonly observed among smaller or poorly managed dark-web services.

There is no authoritative global dataset showing where cybercriminal and hacking forums are physically hosted. Assessments of hosting geography are therefore derived from recurring patterns identified through law-enforcement investigations, underground-market research, passive DNS analysis, bulletproof-hosting studies, and the technical examination of individual platforms.

Russia and parts of the wider Eastern European infrastructure ecosystem are frequently associated with abuse-resistant or bulletproof hosting. Relevant factors may include the presence of specialized providers, inconsistent responses to foreign abuse complaints, jurisdictional barriers, political constraints, and the difficulty of executing foreign preservation, disclosure, or seizure requests. However, this does not establish that most cybercriminal forums are physically hosted, administered or controlled from these countries.

Major cloud and data-center jurisdictions, including the United States and several Western European countries, also appear frequently in forum-related infrastructure. Their presence generally reflects the scale and availability of commercial hosting, cloud platforms, connectivity providers, hosting resellers, reverse proxies, content-delivery networks, and compromised accounts rather than governmental tolerance of cybercriminal activity. Any geographical ranking should therefore be treated as a qualitative representation of recurring infrastructure patterns rather than as a precise measurement of where cybercriminal forums are operated.(Figure 1).

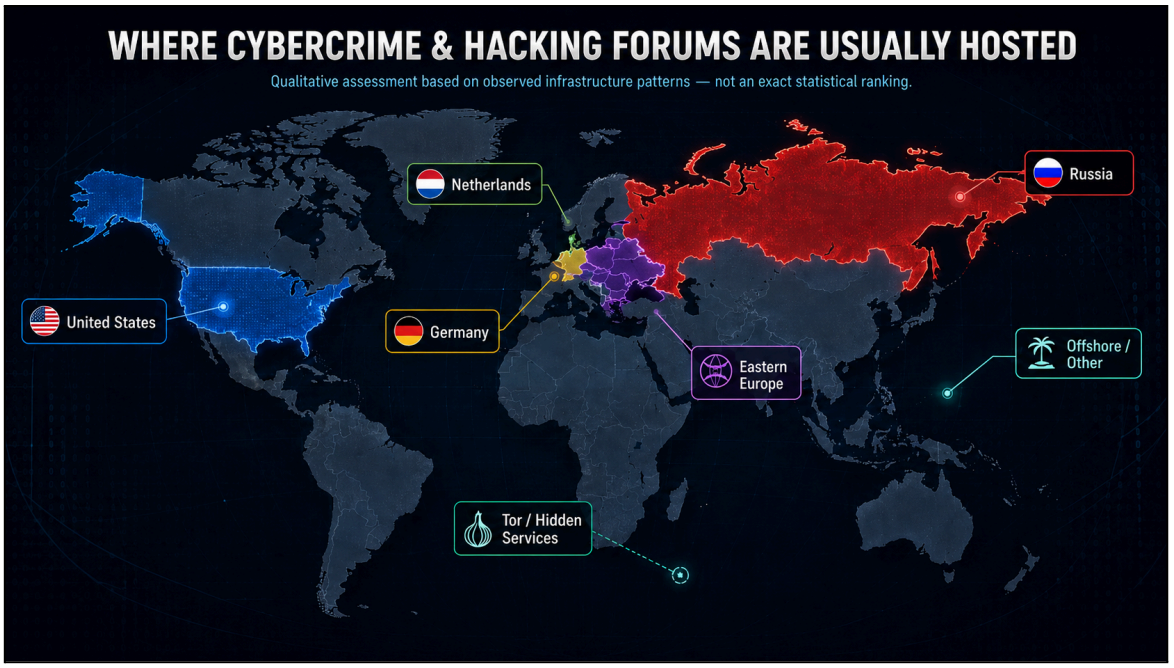


Figure 1 – Common cybercrime forum hosting locations based on investigative and infrastructure analysis

Determining the physical location of a forum is difficult because a single platform may rely on infrastructure distributed across several jurisdictions. Its public-facing server, reverse proxy, content-delivery network, backend database, registrar, payment infrastructure, and administrative personnel may each be located in different countries. Tor hidden services, mirror domains, CDN protection, and layered hosting arrangements can further obscure the origin server. Consequently, the country associated with an IP address or domain record may represent only one technical layer of the platform rather than its actual operational base.

Dark-web forums provide stronger location-obscuring and anonymity benefits, but anonymity does not automatically create operational stability. Onion services may experience prolonged downtime due to denial-of-service attacks, infrastructure failures, hosting problems, misconfiguration, administrator disappearance or internal disputes. Users may also have difficulty distinguishing legitimate replacement addresses from phishing sites, fraudulent mirrors, or impersonation attempts.

Dark-web ecosystems have historically been affected by exit scams, sudden closures, administrator conflict, impersonation, and competition between rival platforms. These factors can shorten the visible lifespan of individual services and accelerate fragmentation across criminal communities. Repeated law-enforcement disruptions and marketplace failures have further encouraged actors to distribute their activity across multiple forums, messaging platforms, and private groups.

The distinction is therefore best understood as one between platform anonymity and platform resilience. A dark-web address may provide additional concealment, but a well-managed forum operating through conventional domains may be more resilient if it maintains stronger infrastructure, reliable backups, distributed administration, and several mechanisms for redirecting users after disruption. Some established communities maintain both conventional domains and Tor mirrors in order to combine accessibility, anonymity, and redundancy.

This remains a general tendency rather than an absolute rule. Highly established dark-web platforms can remain operational for years, while clear-web forums may disappear rapidly following arrests, hosting suspensions, domain seizures or internal collapse. Stability depends less on the network alone than on administrative competence, financial resources, backup availability, distribution of authority, infrastructure redundancy, and the ability to communicate verified replacement addresses to trusted members.

For intelligence purposes, analysts should therefore avoid equating technical location with criminal capability, legitimacy, or durability. A platform’s significance is better assessed through its administration, user community, vendor quality, transaction activity, access controls, infrastructure redundancy, and ability to recover from disruption.

1.3 Registration, Access, and Membership

Access requirements provide important insight into a forum's security posture, organizational culture, and intended membership. However, they should not be treated as definitive indicators of criminal significance. Some highly active cybercriminal forums operate with relatively open registration, while smaller or less influential communities may impose strict entry requirements to create an appearance of exclusivity (Figure 2).

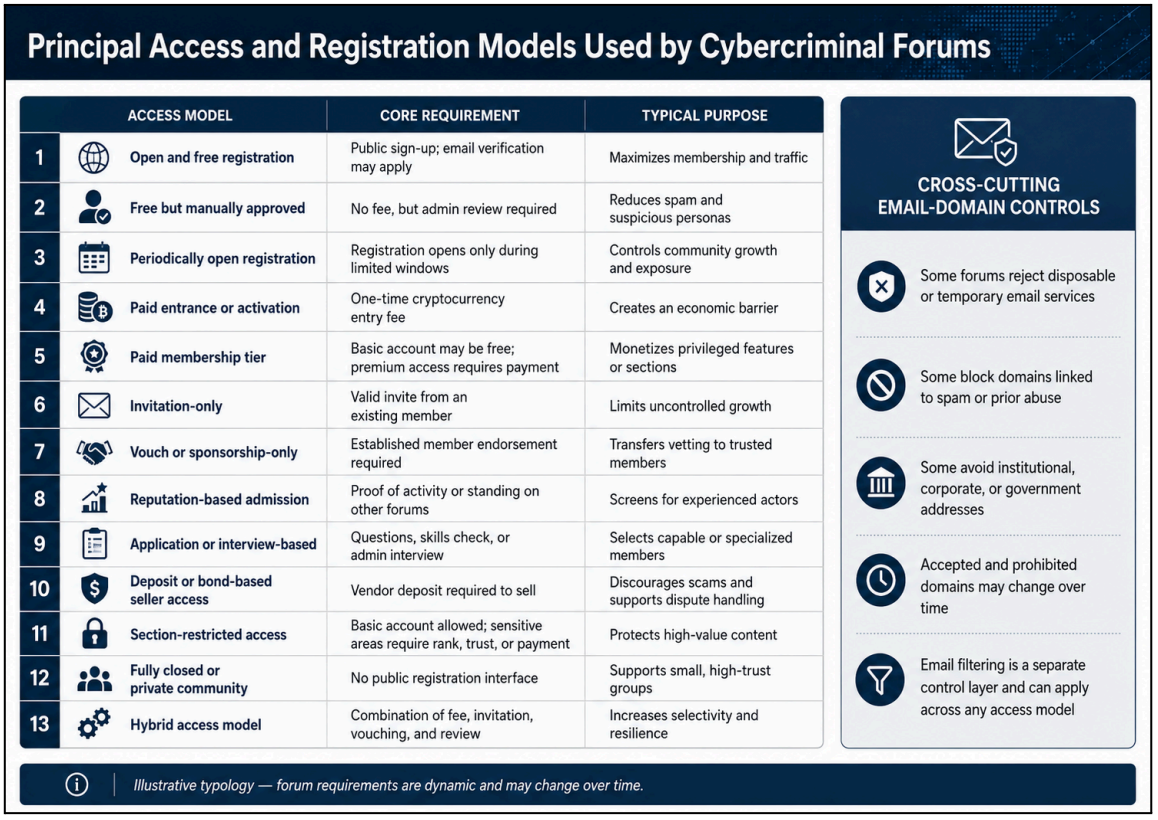


Figure 2 - Main Access types to register to cybercriminal/hacking forums

Forums range from openly accessible platforms to restricted communities requiring registration fees, invitations, sponsorship, interviews or evidence of previous technical or criminal activity. Open registration supports rapid growth, increases potential revenue, and facilitates recruitment, but it also exposes the forum to scammers, inexperienced users, security researchers, and law-enforcement personnel (Figure 3).

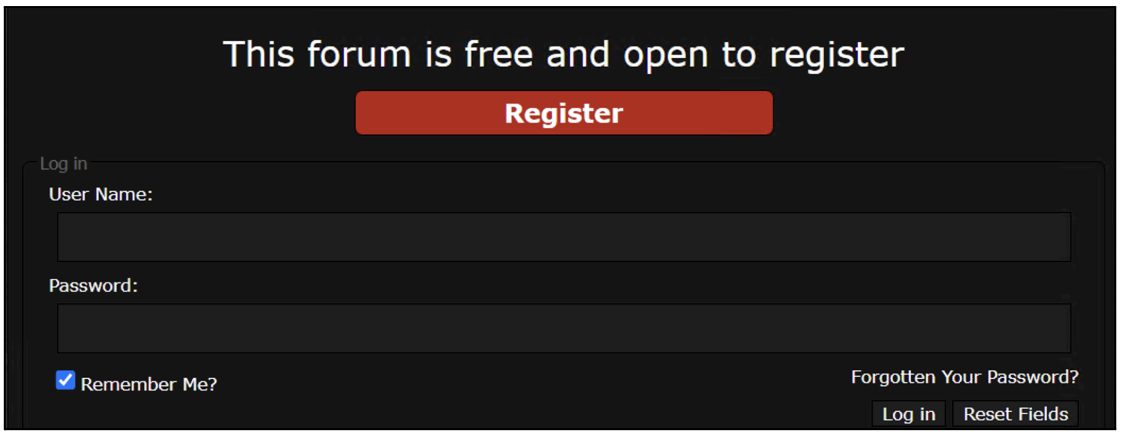


Figure 3 - A free registration on a carding forum (Source: Crdclub forum)

Restricted registration can reduce this exposure and improve the average member experience or credibility, though it may also limit expansion, liquidity, and commercial activity (Figure 4). Administrators, therefore, attempt to balance growth, profitability, operational security, and membership quality.

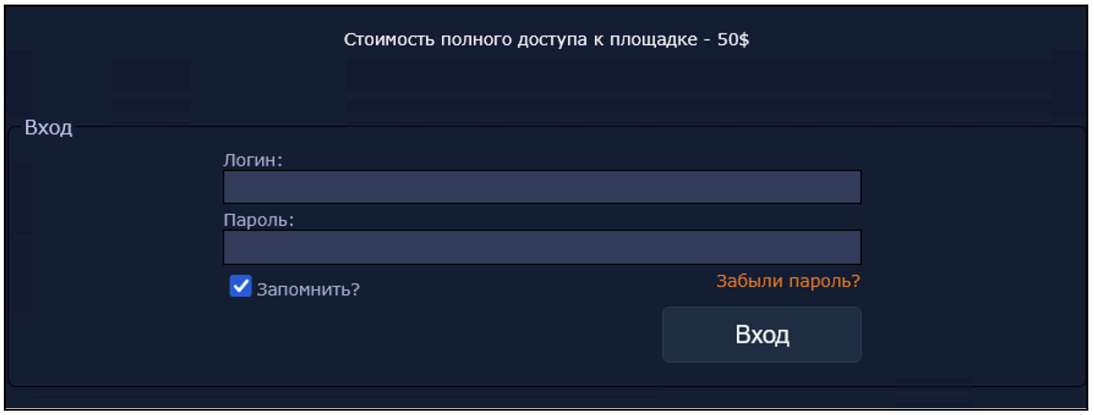


Figure 4 – Restricted forum registration requiring a US$50 fee (source: Verified forum)

Once admitted, members are generally assigned different access levels according to their status, activity, reputation, or commercial role. The terminology varies across platforms, but cybercriminal forums commonly include the following membership categories (Figures 5 and 6).

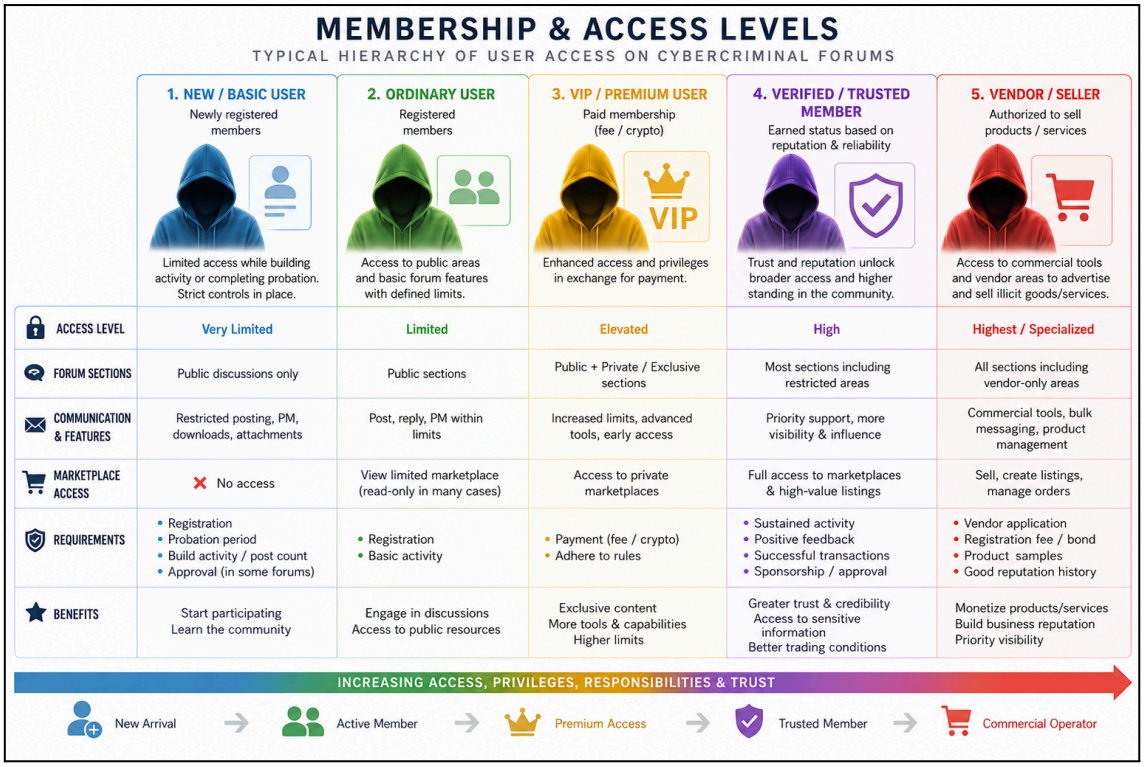


Figure 5 - Common Membership and Access Levels on Cybercriminal Forums

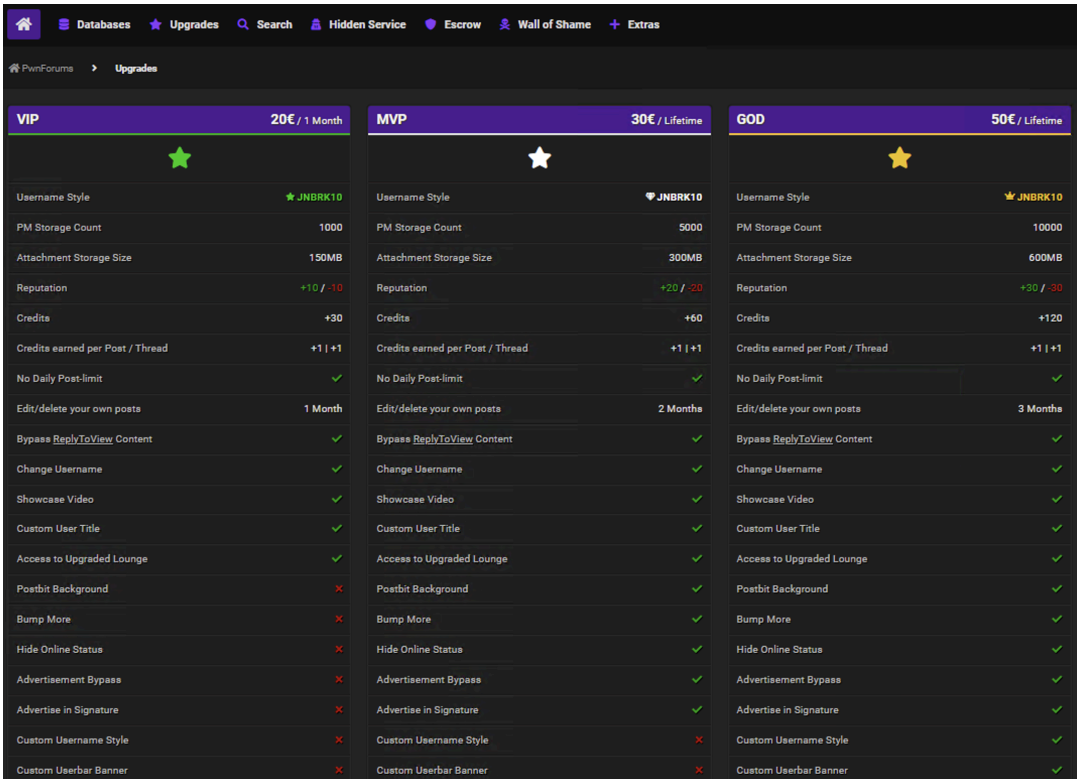


Figure 6 - An example of VIP user packages for sale on a hacking forum (Source: pwndforums)

- **New or Basic User:** This category includes recently registered members whose access and functionality may be restricted. New users may be limited to public discussion areas and may face controls on posting, private messaging, downloading files, or creating commercial advertisements. Some forums require them to complete a probationary period, reach a minimum level of activity, or receive approval from existing members before granting additional privileges.

- **Ordinary User:** Ordinary users represent the majority of registered members. They can generally access the forum's public sections, participate in discussions, respond to posts, and communicate with other members within defined limits. However, they may be unable to access private marketplaces, restricted intelligence sections, premium resources or vendor-only channels.

- **VIP or Premium User:** VIP users receive enhanced access and additional privileges, usually in exchange for a membership fee or cryptocurrency payment. Benefits may include access to private sections, exclusive discussions, premium tools, restricted databases, early access to content or increased posting and messaging capabilities. VIP status should not automatically be interpreted as evidence of expertise or trustworthiness, as it may simply indicate that the member has paid for a higher level of access.

- **Verified or Trusted Member:** Verified or trusted members have usually demonstrated sustained activity, reliability or credibility within the community. This status may be awarded following successful transactions, positive feedback, meaningful contributions, sponsorship by established members or approval by forum administrators. Trusted status generally carries more evidential value than paid VIP status, although it remains dependent on the integrity of the forum's reputation system.

- **Vendor or Seller:** Vendors are members authorized to advertise and sell products or services through the forum. Depending on the platform, prospective vendors may be required to pay a registration fee, provide a security deposit, submit product samples, pass a verification process or demonstrate a history of successful transactions. Vendors may offer stolen data, compromised accounts, malware, network access, financial information, fraud services, or other illicit goods and capabilities. Vendor status is therefore both a commercial function and a specialized access category.

Membership tiers directly influence what an external observer or researcher can see. Newly registered users may encounter only general discussions, outdated material, or low-level advertisements, while established, trusted or paying members may gain access to private marketplaces, specialist sections, vendor channels, and higher-value criminal content. Consequently, a lack of visible activity should not automatically be interpreted as evidence that a platform is inactive or insignificant; it may instead reflect the observer's limited access.

Access policies can also reveal elements of the platform's threat model. A forum that prohibits particular nationalities, victim locations, political topics or forms of criminal activity may be attempting to reduce law-enforcement attention, avoid targeting domestic interests or prevent conflict with actors operating from a particular jurisdiction. Such restrictions should be treated as indicators of operational risk management and community norms rather than conclusive evidence of state protection or official tolerance.

For analysts, the method through which access was obtained has important implications for source reliability, operational security, and legal exposure. Passive observation of openly accessible material differs substantially from entering a community through misrepresentation, obtaining sponsorship under false pretenses, purchasing illegal goods or engaging directly in operational conversations. Collection planning must therefore distinguish between what is technically possible and what is legally, ethically, and organisationally authorized.

1.4 Law-Enforcement Disruption and Forum Reconstitution

International law-enforcement agencies have increasingly targeted cybercriminal forums through coordinated arrests, server and domain seizures, undercover investigations, and the collection of user, communication, and transaction data. One prominent example is BreachForums, an English-language forum used for trading and publishing stolen data. Its founder and chief administrator, Conor Brian Fitzpatrick, was arrested in March 2023. At the time, the platform claimed more than 340,000 members, although this figure should not be interpreted as a verified count of unique or active users. Fitzpatrick was subsequently convicted and, following resentencing in September 2025, received a three-year prison sentence. Despite the closure of the original platform, later forums adopted the BreachForums name and attempted to reconstitute parts of its community, branding, and marketplace functions through replacement domains and infrastructure (Figure 7).



Figure 7 - A forum seized by several international law enforcement agencies

Forum disruption continued beyond BreachForums. In January 2025, an international operation dismantled the Cracked and Nulled platforms, which, together, were reported by US authorities to have more than 9 million registered users, over 4 million on Cracked and over 5 million on Nulled. In March 2026, US authorities also announced the seizure of the LeakBase database and forum infrastructure, which allegedly supported more than 142,000 members and contained a large archive of stolen databases and credentials. These operations demonstrate the increasing law-enforcement focus on high-volume platforms that combine community functions, stolen-data trading, and cybercrime-as-a-service.

Such operations can cause substantial immediate disruption. They remove infrastructure, undermine confidence, interrupt transactions, and create uncertainty about whether law enforcement has obtained private messages, account records, cryptocurrency information, or administrator databases. They may also fracture a community by removing central figures who acted as guarantors, dispute mediators, or custodians of the forum's reputation system.

However, the seizure of a forum should not automatically be interpreted as the elimination of the underlying criminal community. Forums are not merely websites; they are combinations of relationships, reputations, technical assets, communication channels, and shared commercial interests. When these relationships survive, the community may reassemble even if the original platform is lost.

One of the clearest examples followed the seizure of RaidForums. BreachForums was launched shortly afterward and quickly became a major successor platform serving a similar community of stolen-data users. U.S. court records later described BreachForums as having emerged as a replacement for RaidForums and noted that it rapidly grew into one of the largest English-language hacking forums. This illustrates how law-enforcement disruption may remove a particular platform without eliminating the demand, vendors, or social networks that made it valuable.

Forum reconstitution can occur through several mechanisms. Remaining administrators may restore a backup of the original database, recreate the platform under a new domain, or establish a replacement site under a different name. Moderators or senior members may also seek to maintain continuity with the previous forum and transfer its users, vendors, and reputation structures to a successor platform. In other cases, several competing replacements appear, each claiming to be the legitimate continuation of the seized community.

The arrest of only part of a forum's management team is particularly unlikely to guarantee permanent closure when authority and technical access are distributed. Other administrators, moderators, or infrastructure operators may retain database backups, source code, cryptocurrency reserves, member contact lists or access to external communication channels. These individuals may keep the original forum operational, move it to a replacement domain, or rebuild it after a short interruption.

A forum may consequently reappear:

- under the same name but through a different domain or onion address;
- under a modified name intended to signal continuity;
- as a new platform operated by former administrators or moderators;
- through a restored database containing previous accounts and posts;
- or as a looser community initially organized through Telegram, Jabber or another encrypted messaging service before a full forum is rebuilt.

The speed and credibility of the recovery depend heavily on whether surviving team members can prove that the replacement is genuine. Criminal communities are highly vulnerable to impersonation after a seizure. Law-enforcement-controlled domains, phishing pages, and fraudulent successor sites may all appear plausible. Administrators, therefore, use signed messages, established communication accounts, recognized pseudonyms, and endorsements from trusted vendors to authenticate a replacement platform.

This creates a recurring cycle of disruption, fragmentation, and reconstitution. Law enforcement removes infrastructure and arrests key personnel; users disperse across alternative forums and messaging channels; surviving administrators or competitors establish successor platforms; and vendors gradually rebuild their reputations and customer bases. The reconstituted forum may retain the same brand because the name retains criminal market value, or adopt a new identity to distance itself from compromised infrastructure.

Law-enforcement action remains operationally significant even when a forum later returns. A seizure can expose users, destroy trust, reduce transaction volume, force actors to adopt less efficient channels, and create opportunities for further intelligence collection. Repeated disruptions also impose financial and organizational costs on administrators and vendors. The analytical mistake is not to regard takedowns as ineffective, but to treat the loss of a domain as equivalent to the loss of an ecosystem.

For intelligence purposes, forum continuity should therefore be evaluated across several layers:

- **Technical continuity:** whether the same database, software, hosting infrastructure or cryptocurrency wallets are being reused.
- **Administrative continuity:** whether former administrators, moderators or guarantors remain involved.
- **Identity continuity:** whether established vendors and members retain their aliases, reputation and transaction histories.
- **Community continuity:** whether the previous user base migrates to the replacement platform.
- **Market continuity:** whether the same products, services and criminal relationships continue to be offered.

A successor forum that uses a different name and domain may still represent substantial continuity if it is operated by the same personnel and serves the same vendors. Conversely, a platform using the original name may have little genuine connection to the earlier forum and may instead be an impersonation, scam or law-enforcement-controlled environment.

The resilience of cybercriminal forums, therefore, originates not only from technology but from the portability of criminal relationships. Domains can be seized, servers confiscated, and administrators arrested, but trusted identities, customer networks, and commercial demand can migrate. Effective analysis must follow the actors and relationships across platforms rather than treating each domain as an isolated entity. The forum is the visible interface; the more durable structures are the community and the market operating behind it.

2. How Cybercriminal Forums Operate

2.1 Administration and Governance

Cybercriminal forums require governance because anonymity, illegality, and limited legal recourse create persistent incentives for fraud, deception, and internal conflict. Administrators and moderators, therefore, function as the leadership of an unregulated criminal institution. They establish membership rules, organize content, verify vendors, regulate advertising, resolve disputes, and determine which actors remain credible enough to participate in the community.

The most important asset controlled by a forum's leadership is not the underlying software or hosting infrastructure, but the community's confidence in the platform. Forums depend on participants believing that rules will be applied consistently, escrow funds will not be stolen, and fraudulent vendors will be sanctioned. Once members suspect that administrators are manipulating disputes, favoring particular sellers, misappropriating deposits, or preparing an exit scam, confidence can deteriorate rapidly. Governance consequently performs both a security function, by limiting disruptive and fraudulent behavior, and a commercial function, by making criminal transactions appear sufficiently reliable to attract buyers, vendors, and advertisers. The public leadership structure may include several specialized roles (Figure 8)

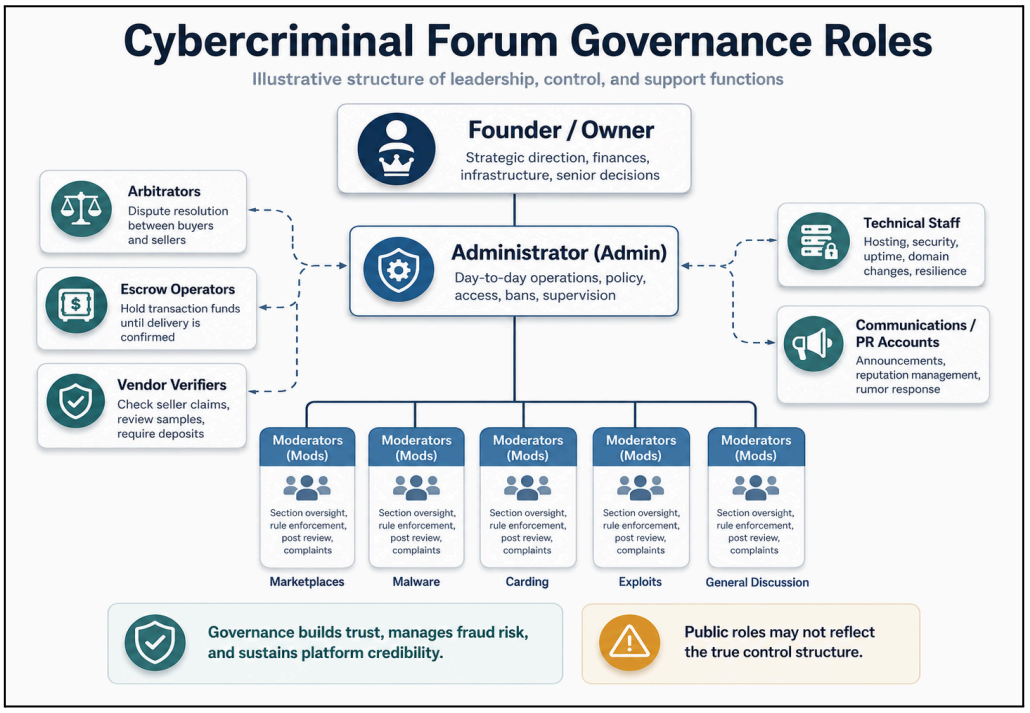


Figure 8 - Management Roles Within Cybercriminal Forums

- **Founder or owner:** The founder or owner exercises ultimate control over the platform and determines its strategic direction. This individual may oversee finances, infrastructure, senior appointments, security policies and the forum's long-term commercial development. In smaller communities, the founder may also operate as the principal administrator, moderator or escrow operator. In more mature forums, ownership may be deliberately concealed behind several administrative personas.

- **Administrator, or "admin":** Administrators manage the forum's day-to-day operations and translate the owner's strategic decisions into practical policies. Their responsibilities may include controlling user permissions, supervising moderators, approving vendors, managing advertising, enforcing access restrictions, and making final decisions concerning bans, disputes, and commercial partnerships. Senior administrators may also control the forum's cryptocurrency wallets, escrow systems, and relationships with external service providers (Figure 9).

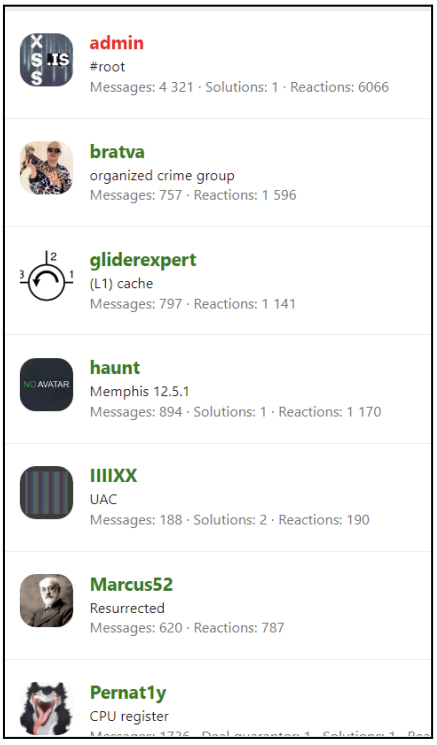


Figure 9 - List of Admin and moderators on a Russian hacking forum (Source: XSS Forum)

- **Moderator, or "mod":** Moderators enforce rules and supervise user activity. Larger forums commonly assign moderators to particular sections, such as malware, stolen databases, compromised accounts, financial fraud or hacking services. They may review posts, remove prohibited content, address complaints, sanction users, and intervene in disputes. Moderators also help maintain the quality and organization of forum content, which is important for sustaining user engagement and commercial activity.

In some cases, moderators are recruited directly from the forum's established membership, typically based on their reputation, technical knowledge, activity level, and demonstrated loyalty to the community (Figure 10).



Figure 10 - Moderator recruitment post on a carding forum (Source: Altenen forum)

- **Arbitrator:** Arbitrators adjudicate disputes between buyers, sellers and service providers. They may review transaction records, private messages, delivery evidence, and technical samples before determining whether a refund, compensation or sanction is justified. The perceived neutrality of arbitrators is critical, as biased or inconsistent decisions can undermine confidence in the entire marketplace.

- **Escrow operator:** Escrow operators temporarily hold transaction funds until both parties confirm that the agreed product or service has been delivered. Escrow reduces the risk of direct fraud, but it also concentrates considerable financial power in the hands of the forum's leadership. The misuse of escrow deposits is therefore one of the principal risks facing forum participants.

- **Vendor verifier:** Vendor verifiers assess whether sellers possess the products, access or capabilities they claim to offer. Verification may involve examining samples, reviewing previous activity, requiring a financial deposit or conducting controlled transactions. Verification does not guarantee legitimacy, but it raises the cost of creating fraudulent vendor identities and provides administrators with an additional source of revenue.

- **Technical staff:** Technical personnel maintain hosting, software, security, availability, and resilience against denial-of-service attacks or law-enforcement disruption. They may manage domain changes, backup infrastructure, encryption, authentication mechanisms, and migration between clearnet, Tor, and alternative communication platforms.

- **Communications or public-relations accounts:** Some forums use dedicated accounts to publish announcements, address rumors, communicate infrastructure changes, and maintain relationships with users on external platforms. These accounts become particularly important during periods of disruption, data leakage, law-enforcement action or internal controversy.

Although these roles may appear clearly differentiated, cybercriminal governance is rarely transparent. A single individual may operate several administrative identities to exaggerate the size or professionalism of the management team. Apparent moderators may in reality be business partners, employees, affiliates or compromised accounts controlled by other actors. Ownership may also change without public acknowledgment, particularly following internal disputes, arrests, infrastructure seizures, or private sales of the forum.

Analysts should therefore distinguish between the forum's declared governance structure and its probable underlying control structure. Public titles indicate how authority is presented to the community, but they do not necessarily reveal who controls the infrastructure, financial accounts, databases or strategic decisions. This distinction is important because the visible administrator may be only a spokesperson, while another actor controls the forum's wallets, servers or access credentials.

Administrative behavior can provide valuable insights into a forum's internal conditions and strategic direction. Sudden rule changes, withdrawal restrictions, higher vendor deposits, aggressive fundraising, unusual escrow delays, staff resignations, or unexplained downtime may indicate financial stress, internal conflict, compromise, law-enforcement pressure, or preparation for an exit scam. Public disputes between administrators and moderators may expose rival factions or competing commercial interests.

Changes in moderation policy may also reveal strategic repositioning. A forum that begins permitting ransomware recruitment, initial-access sales or data-extortion services may be attempting to attract more sophisticated and profitable actors. Conversely, a platform that prohibits ransomware discussions, bans politically sensitive activity, or restricts transactions involving particular countries may be seeking to reduce law-enforcement attention or preserve relationships with local authorities.

Governance should therefore be examined not merely as an organizational feature, but as an intelligence indicator. The composition of the administrative team, the consistency of enforcement, the handling of disputes, and the movement of funds can reveal the forum's stability, commercial priorities, risk tolerance, and vulnerability to disruption.

2.2 Trust and Reputation

Trust is the central economic problem of the criminal underground. Participants use pseudonyms, cannot rely on the courts, and operate in an environment where deception is the norm. Reputation systems are designed to reduce but never eliminate this uncertainty. Reputation can derive from account age, transaction reviews, forum rank, endorsements, verified deposits, previous work, and relationships with respected members. The strongest reputation is usually cumulative and cross-platform. An actor known for several years, vouched for by established users and linked to completed transactions, carries more weight than a recently created account with numerous unverified claims. However, reputation is vulnerable to manipulation. Accounts can be sold, stolen or shared. Reviews can be fabricated. Vendors may conduct small legitimate transactions to build credibility before committing large-scale fraud. Established actors may also use a reputable identity to promote a new and less trustworthy service.

A robust assessment should distinguish between:

- **Platform-assigned reputation**, such as rank or badges.
- **Customer-generated reputation**, such as reviews and dispute outcomes.
- **Peer reputation**, including endorsements from established actors.
- **Externally validated reputation**, based on activity observed elsewhere.
- **Technical credibility**, demonstrated through samples or verifiable claims.

Negative information is often more revealing than positive feedback. Disputes can expose delivery methods, payment addresses, communication patterns, operational failures, and relationships between actors. Even an apparently minor complaint may reveal the actual nature of a service. Reputation should therefore be analyzed as a network of claims rather than a score. The key question is not “Does this vendor have a high rating?” but “Which independent observations support the conclusion that this identity controls the claimed capability?”

2.3 Transactions and Criminal Business Models

Transactions conducted through cybercriminal forums range from straightforward purchases to complex, long-term commercial relationships involving subscriptions, licensing, profit sharing, brokerage, or long-term service provision. The commercial model generally reflects the nature of the commodity, the degree of operational support required, and the level of trust between the parties. A stolen database may be sold for a fixed price or auctioned to several bidders, while malware, attack infrastructure, and fraud-enabling services are increasingly provided through recurring or usage-based arrangements.

Europol describes a cybercrime economy in which stolen information is repeatedly packaged, traded, and exploited across interconnected platforms, allowing the same underlying compromise to generate revenue for several actors at different stages of the criminal supply chain. Common transaction models include:

- Fixed-price sales of data, credentials, accounts, tools or access.
- Auctions for exclusive or time-sensitive datasets and network access.
- Subscription-based access to malware, databases, intelligence feeds or criminal services.
- Pay-per-use access to botnets, proxies, phishing infrastructure and other malicious resources.
- Affiliate arrangements in which developers and operators divide proceeds from successful attacks.
- Commission-based cash-out, laundering and cryptocurrency-conversion services.
- Rental or licensing of malware, often accompanied by updates and technical support.
- Brokerage fees for introductions between buyers, sellers and specialist service providers.
- Escrow-protected transactions involving a forum administrator or trusted guarantor.
- Direct private sales to established customers outside the forum's visible marketplace.

The distinction between a criminal product and a criminal service has consequently become increasingly blurred. Malware may be licensed rather than sold outright and can include access to management panels, infrastructure, regular updates, evasion maintenance, and customer support. Recent research into crypter services found that their value often depended on continuous renewal and sustained antivirus evasion rather than the delivery of a single static tool. Stolen credentials may similarly be distributed through searchable platforms, while fraud packages can combine identity documents, payment accounts, operational instructions, technical tools, and direct human assistance. This professionalization enables customers with limited technical knowledge to consume complex criminal capabilities as managed services.

2.3.1 Forum Owners as Commercial Intermediaries

Forum owners and administrators are not merely passive hosts. On commercially developed platforms, they may operate as intermediaries that regulate access, monetize visibility, facilitate transactions, and generate revenue from economic activity within the community. The precise model varies significantly: some forums are relatively informal discussion communities, while others closely resemble managed marketplaces with membership tiers, vendor programs, escrow systems, and advertising products.

One common source of revenue is paid membership. Users may pay registration charges or purchase elevated account levels that provide access to restricted sections, increased messaging allowances, reduced posting limitations, enhanced search functions, or access to valuable leaked material. RaidForums, for example, was reported to have generated revenue through advertisements and tiered membership accounts that gave users greater access to forum content. Paid membership can serve two purposes simultaneously: generating income for the administrators and creating an initial barrier against low-effort participants, automated accounts, and some forms of infiltration. Forums can also generate revenue through advertising and promotional placement. Vendors may pay for banner advertisements, prominent marketplace positions, pinned threads, highlighted listings or permission to promote external services.

Advertising is particularly valuable to providers of mixers, hosting services, proxy networks, cryptocurrency exchanges, malware services, and identity-verification or “checking” services seeking direct access to a concentrated criminal customer base. Research into Russian-language forums identifies advertising, commercial partnerships, paid account status, registration fees, escrow, and security deposits among recurring sources of administrator income.

Another important revenue stream is vendor accreditation and status selling. A forum may require sellers to pay a fee or lodge a refundable security deposit before receiving verified-vendor status. These mechanisms are intended to discourage low-value fraud and provide limited compensation when a seller defaults, though their effectiveness depends entirely on the administrator's integrity. Paid status can also improve the seller’s visibility and credibility, meaning that what appears to be a trust mechanism may simultaneously function as a commercial product sold by the forum.

Escrow and guarantor services provide both transaction security and income. Under a typical escrow arrangement, the buyer transfers payment to an administrator, automated system, or recognized guarantor. Funds are released once the buyer confirms delivery or the agreed conditions are satisfied. If a dispute arises, moderators may examine messages, samples, and transaction terms before determining whether funds should be released or returned.

Published research has documented escrow charges ranging from a percentage of the transaction to minimum fixed fees, although rates differ considerably by forum, deal size, and perceived risk. The founder of BreachForums was also alleged by US authorities to have offered a trusted middleman or escrow service to facilitate transactions between forum members.

Escrow gives the forum owner a privileged position. Administrators can observe counterparties, transaction values, wallet addresses, disputes and the types of products being exchanged. This provides commercial influence but also creates legal and operational exposure: rather than simply providing a communication platform, administrators may become directly involved in facilitating, arbitrating and profiting from illicit transactions. Escrow reserves and vendor deposits can also expose the forum to exit fraud if an administrator disappears with funds, or to seizure if law enforcement gains control of the platform's wallets or financial infrastructure. Additional revenue sources may include:

- Fees for posting or renewing commercial advertisements.
- Payments to pin, highlight or "bump" sales threads.
- Fees for changing usernames or restoring suspended accounts.
- Paid access to premium databases, leak repositories or automated checking tools.
- Sponsorship and referral arrangements with external criminal services.
- Commission from automated marketplaces integrated into the forum.
- Fees for dispute arbitration, identity checks or seller verification.
- Donations or voluntary contributions from established members.

These models should not be assumed to exist uniformly across all forums. Some communities prohibit open advertising or charge no transaction commission because their strategic value lies in exclusivity, intelligence exchange or relationships between high-level actors. Others derive most of their income from membership and advertising rather than taking a percentage of sales. Analysts should therefore distinguish between forum-wide revenue mechanisms, administrator-operated services, and transactions negotiated independently between users.

2.3.2 Trust, Escrow, and Transaction Risk

Escrow reduces counterparty risk but does not eliminate it. Buyers remain vulnerable to outdated datasets, fraudulent samples, overstated access, hidden exclusivity arrangements, and administrators colluding with sellers. Sellers may face charge disputes, replacement demands, or buyers who attempt to exploit the arbitration system. In response, mature forums may require transaction records, proofs of ownership, samples, or confirmation through a designated guarantor. Research into cybercrime service markets shows that escrow, guarantors, reputation systems and security deposits form part of a wider governance structure that supports recurring commercial activity. The forum's reputation is therefore an economic asset in itself. Administrators must balance revenue generation against the need to limit blatant fraud. A platform that permits unrestricted scamming may gain short-term registration and advertising income but lose credible vendors and high-value buyers. Conversely, strict moderation and reliable arbitration can attract more sophisticated

participants and support higher-value transactions. This creates a form of illicit platform governance in which administrators monetize not only technical access to the forum, but also the trust and perceived order that they maintain.

2.3.3 Pricing and Analytical Interpretation

Pricing can provide useful intelligence, but it is easily misinterpreted. A high advertised price does not necessarily indicate that an offering is genuine, exclusive, or operationally valuable. It may reflect seller expectations, negotiation strategy or deliberate signaling. Conversely, a low price may result from non-exclusive sale, incomplete validation, outdated information, urgent monetization, limited privileges or an attempt to attract multiple buyers.

When assessing the value of network access, stolen data or criminal services, analysts should consider:

- The victim's sector, geography, and revenue.
- The privileges and systems accessible to the seller.
- Persistence and the likelihood that access remains active.
- Network visibility and access to security-management systems.
- Whether access or data is exclusive or sold repeatedly.
- The volume, freshness, and sensitivity of the information.
- The extent of technical or operational support is included.
- The seller's reputation and previous transaction history.
- The use of escrow, guarantees, or replacement conditions.
- Evidence that the seller controls the advertised asset.

Advertised prices should also be distinguished from completed transaction values. Sales posts often represent opening positions rather than final prices, and negotiations may result in substantial discounts, bundled services, or revenue-sharing arrangements that are not visible publicly.

2.3.4 Movement from Public Listings to Private Transactions

The movement of transactions away from the visible forum is normal. Public posts establish interest, reputation, and initial credibility, but sensitive details are frequently exchanged through private messages, encrypted communication applications, or direct contact accounts. This protects victim information and operational methods while reducing the amount of evidence available to competitors, researchers, and law enforcement. Large-scale research into forum behavior also indicates that users often limit explicit criminal disclosure in visible posts and progressively move toward more restricted communication.

As a result, public thread counts, replies, and visible sales confirmations can substantially understate actual transaction volume. Forum-generated revenue may likewise be difficult to calculate because some payments occur through integrated systems, while others are transferred directly between users or moved to Telegram and other communication platforms. Forums remain important for reputation building, escrow and structured commercial discovery even when the final negotiation and payment occur elsewhere.

Visible engagement can also be manipulated. Vendors may post false reservations, use associated accounts to manufacture positive feedback or claim that an item has been sold in order to create scarcity. Administrators themselves may tolerate or participate in such activity when it increases advertising revenue or apparent marketplace liquidity. Consequently, analysts should treat replies, reviews and sales claims as indicators requiring corroboration rather than as proof of completed transactions.

The most important analytical question is often not whether an advertisement appeared or a payment was claimed, but whether the capability was subsequently transferred into operational use. Connecting a forum listing to a later intrusion, fraud campaign, malware deployment, or extortion operation substantially strengthens intelligence confidence. Useful corroboration may include matching victim characteristics, timestamps, wallet activity, technical indicators, reused contact information, unique data samples, or statements by the buyer or seller. This distinction separates marketplace observation from operational intelligence and helps determine whether a listing represents a credible capability, an unsuccessful sale, repeated resale, or simple criminal fraud.

2.4 Forum Infrastructure, Security, and Anonymity

Cybercriminal forums generally rely on conventional web technologies adapted to provide anonymity, access control, and resilience against disruption. Many use self-hosted bulletin board platforms such as XenForo, MyBB, phpBB, or heavily modified equivalents, which provide ready-made features for registration, private messaging, moderation, reputation scoring, paid memberships, and marketplace-style sections. Their familiar interfaces reduce development costs and allow criminal communities to reproduce the structure and usability of legitimate online forums while adding invitation systems, restricted areas, vendor verification, and other controls tailored to illicit activity.

The visible forum is usually only one component of a broader infrastructure. Operators may rely on virtual private servers, dedicated hosting, reverse proxies, traffic-filtering services, and infrastructure obtained through intermediaries or false identities. Because distributed denial-of-service attacks are frequently conducted by rivals, extortionists, and dissatisfied users, and may also coincide with periods of

law-enforcement disruption, many established forums deploy some form of anti-DDoS protection. Users are therefore commonly presented with browser verification pages, JavaScript challenges, CAPTCHA, waiting rooms, or proof-of-work mechanisms before reaching the login page. These controls help filter automated traffic and conceal origin servers, although they may also introduce dependencies on external protection providers and create additional technical indicators for investigators (Figure 11).



Figure 11 – Anti-DDoS browser-verification page displayed by a French-language cybercriminal forum (source: Malekal forum)

Domains and servers are frequently treated as replaceable assets rather than permanent infrastructure. Administrators may maintain reserve domains, backup databases, alternative login pages, and external announcement channels that can be activated following domain suspension, law-enforcement seizure, denial-of-service attacks, or internal disputes. Some forums maintain both a conventional web domain and a Tor onion service. The clearnet version facilitates accessibility, recruitment, and broader visibility, while the Tor version provides an alternative access route and reduces dependence on conventional domain registrars. In some cases, both addresses lead to the same underlying forum and database; in others, sensitive sections or higher-risk activities are restricted to Tor. Updated links are often distributed through Telegram channels, encrypted messaging applications, signed administrator messages, or designated announcement pages. These mechanisms help preserve continuity but also create additional infrastructure, accounts, and communication patterns that can be investigated.

Cybercriminal communities complement these arrangements with layered security measures intended to protect infrastructure, identities, and transactions. Common practices include anonymity networks, encrypted communications, cryptocurrency payments, compartmentalized accounts, invitation-only access, restrictions on sensitive discussion, and limits on the technical or victim information visible to unverified users. Administrators may also require multi-factor authentication, encrypted messaging keys, or signed communications to reduce account hijacking and impersonation.

Security practices vary considerably across forums and between individual actors. A low-level fraud vendor may rely on mainstream messaging platforms, reused usernames, and direct cryptocurrency payments, whereas a high-value access broker may compartmentalize victim information, restrict potential buyers, and avoid publishing evidence that could expose the affected organization or method of compromise. Analysts should therefore avoid attributing a uniform level of sophistication to an entire forum based on the practices of its administrators or most capable members.

Despite these precautions, anonymity remains imperfect. Forum operators and users repeatedly expose themselves through operational mistakes, reused aliases, payment patterns, language habits, overlapping infrastructure, personal relationships, and inconsistent security practices. Long-running forums remain vulnerable to technical investigation, undercover activity, human intelligence, financial tracing, infrastructure analysis, and international law enforcement cooperation. Takedowns may shorten platform lifecycles and force communities to fragment or migrate, but they rarely eliminate the underlying criminal demand or the relationships established through the forum (Figure 12).

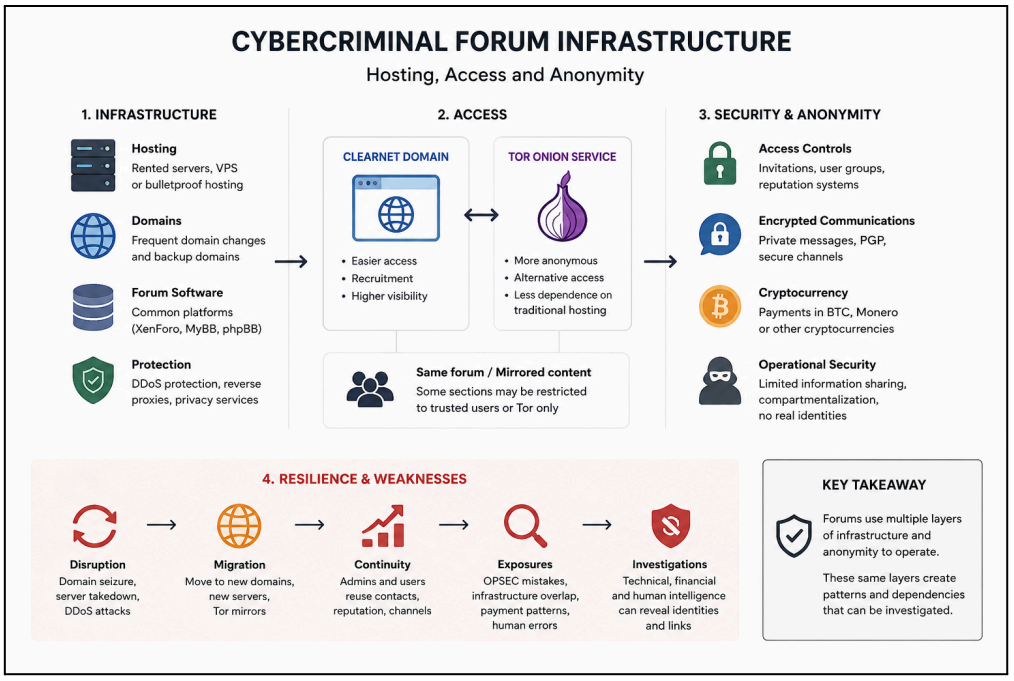


Figure 12 - Cybercrime forums infrastructure overview

From an intelligence perspective, the mechanisms used to preserve anonymity and continuity can themselves generate valuable indicators. Migration notices, signed administrator messages, shared contact accounts, reused cryptocurrency wallets, common encryption keys and recurring infrastructure patterns may help link actors and successor platforms.

Reputation is particularly important during migration: vendors and administrators must demonstrate continuity to retain trust, customers and status. In doing so, they often reproduce identifiers or communication channels that reveal connections between old and new platforms. Forum infrastructure should therefore be assessed not only as a protective layer, but also as an intelligence surface that exposes relationships, dependencies and potential points of disruption.

3. Main Categories of Cybercriminal Forums

Cybercriminal and hacking forums differ significantly in their scope, target audience, and commercial specialization. Some operate as broad, general-purpose marketplaces and discussion platforms where users exchange knowledge, tools, services, and illicit goods across multiple areas of cybercrime. Others are organized around specific languages, countries, or regions, reflecting local criminal networks, cultural norms, payment systems, and targeting priorities. Alongside these broad communities, more specialized forums focus on particular segments of the underground economy, including the sale of network access, compromised accounts and leaked data; carding, financial fraud and identity crime; and hacking, malware development and cyberattack services. Examining these categories is essential because each type of forum supports a different stage of the cybercriminal value chain, from initial access and data acquisition to fraud, exploitation, monetization, and the delivery of complete attack capabilities (Figures 13 and 14).

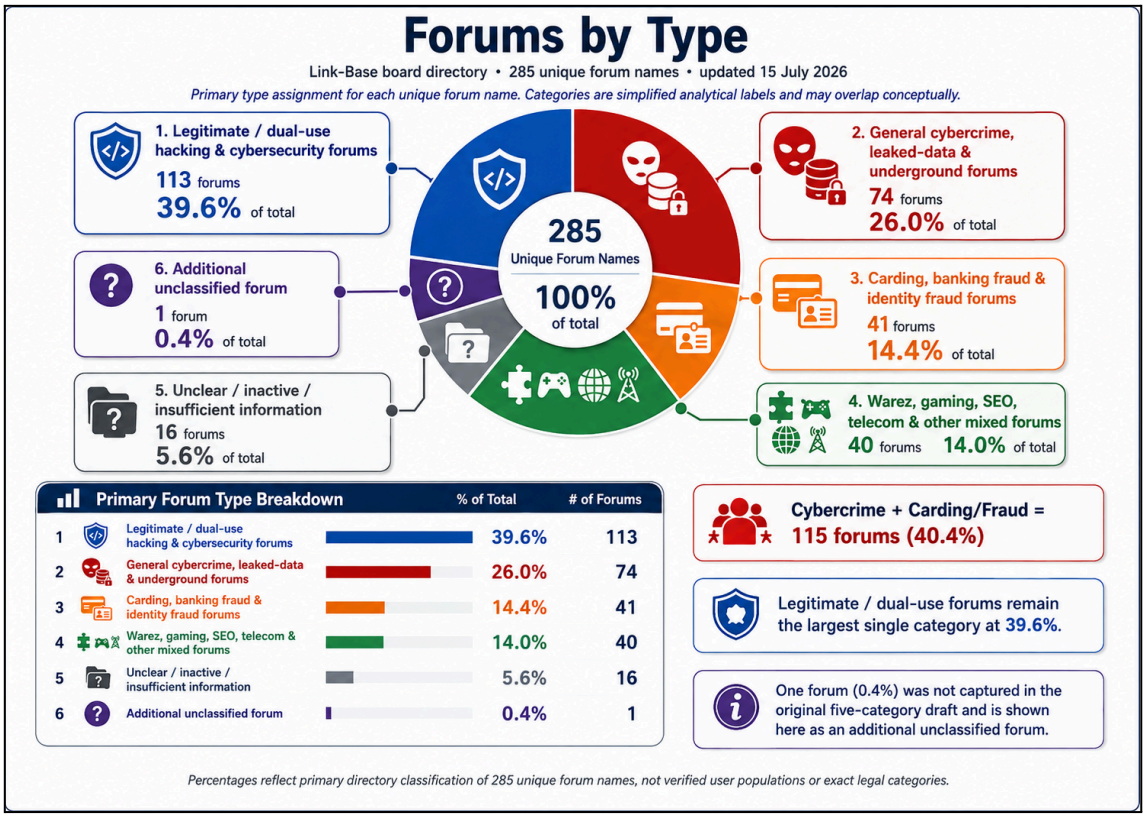


Figure 13 - Cybercrime forums statistics by type (Source:Link-base forums repository)

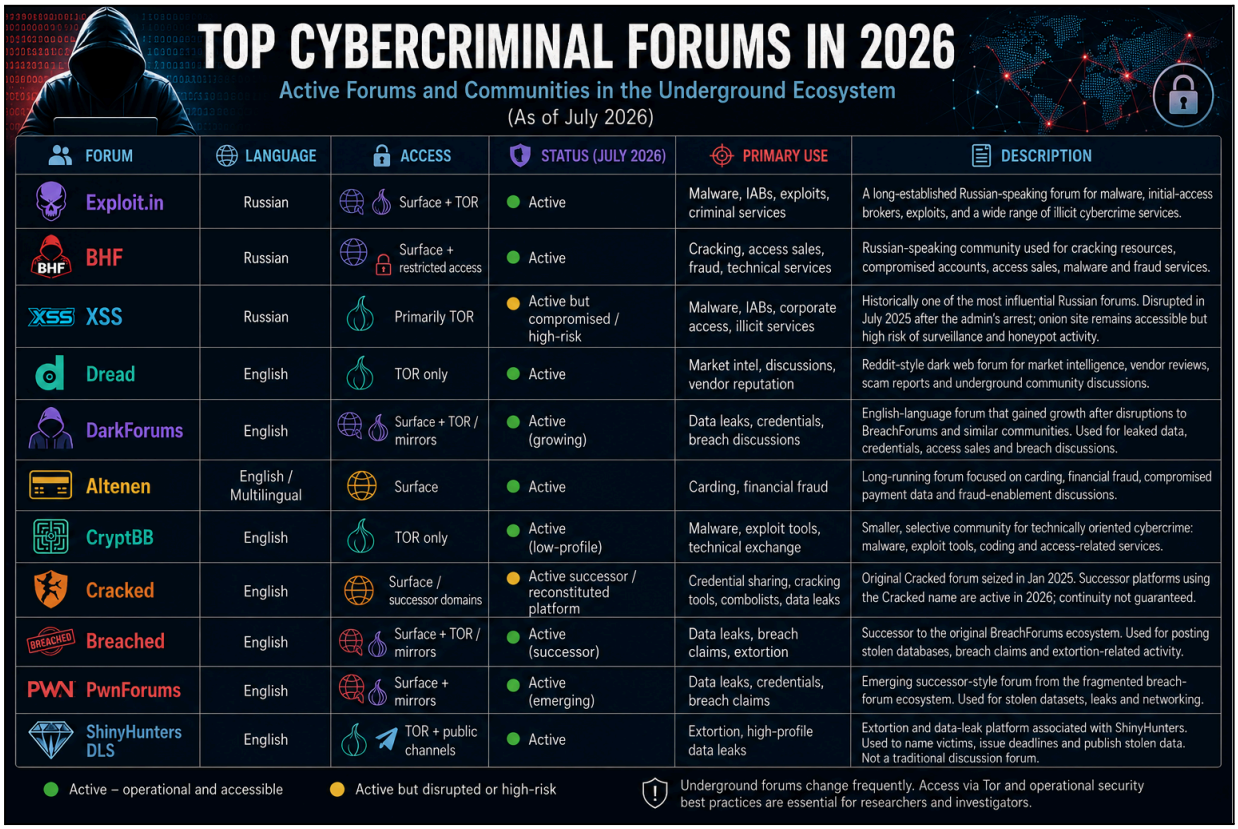


Figure 14 - Top Cybercriminal forums in 2026

3.1 General Forums

General cybercrime forums are broad criminal platforms that host a range of illicit activities within the same environment. Rather than focusing on a single service or criminal method, they bring together vendors, buyers, technical specialists, fraudsters, access brokers, malware developers and relatively inexperienced users. Their importance lies in their ability to connect different parts of the cybercriminal ecosystem and facilitate movement between distinct criminal activities.

These forums frequently contain sections dedicated to compromised accounts, stolen data, malware, financial fraud, social engineering, cryptocurrency, hacking services and operational tutorials (Figure 15). However, the presence of a category does not necessarily mean that the platform contains high-quality or sophisticated activity in that field. General forums usually combine professional criminal services with low-level discussion, recycled tools, fraudulent advertisements and inexperienced participants.

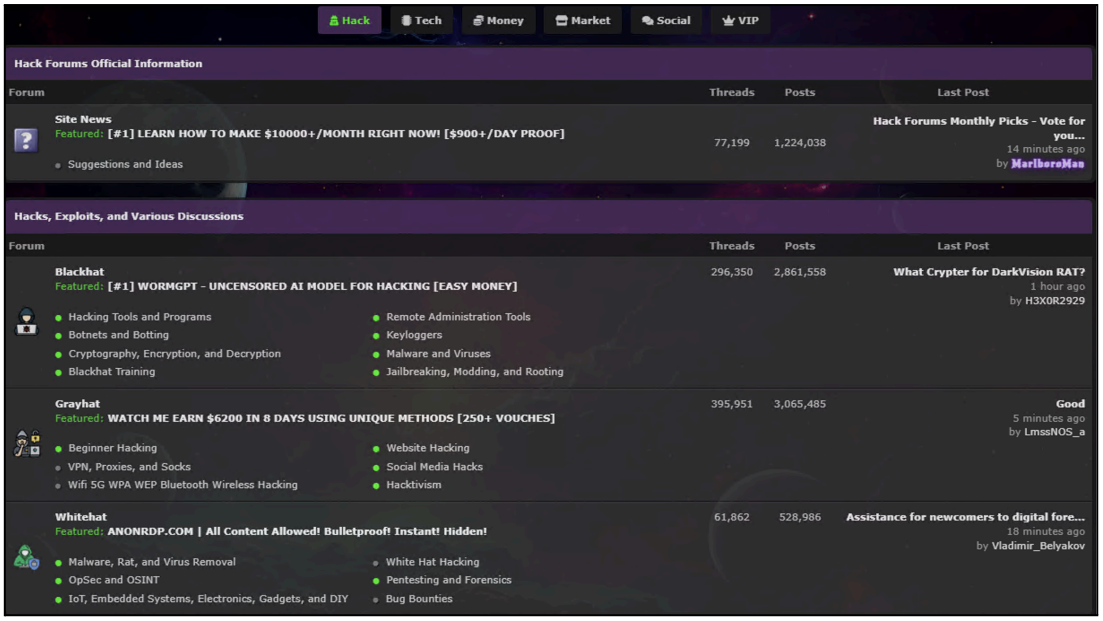


Figure 15 - A general hacking forum (Source: hackforums)

The analytical value of a general cybercrime forum therefore, depends less on its total membership than on the quality of the actors and commercial activity operating within it. A forum with a large number of registered users may contain relatively limited meaningful criminal trade, while a smaller platform may host trusted vendors or specialized brokers with direct access to high-value targets. General forums perform several functions within the criminal ecosystem:

- They provide entry points for new or less experienced offenders.
- They allow vendors to advertise services to a broad customer base.
- They enable actors from different criminal specializations to identify partners.
- They support reputation building through reviews, disputes, and completed transactions.
- They provide knowledge-sharing environments where techniques, tools, and operational experience are exchanged.
- They serve as recruitment spaces for affiliates, developers, money mules, intrusion specialists, and other service providers.

These forums also act as bridges between low-level and advanced criminal environments. New participants may begin by accessing tutorials, purchasing basic tools, or conducting small-scale fraud. More capable users can gradually establish reputations, develop relationships, and gain access to restricted sections or private groups. The forum, therefore, functions not only as a marketplace but also as a mechanism of criminal progression and professionalization.

From an intelligence perspective, general forums provide broad visibility into changes in criminal demand and supply. Increased discussion of a particular vulnerability, authentication method, financial institution, or technology may indicate growing criminal interest. However, the volume of content also produces significant noise. Monitoring should consequently focus on specific actors, commercial sections, disputes, recruitment activity, and services that align with defined intelligence priorities. It is also important to understand that much of the most sensitive activity may not occur directly on the forum. Vendors frequently use public threads to establish credibility and attract customers, before moving negotiations and delivery to private messages or encrypted communication platforms. General cybercrime forums should therefore be viewed as visible coordination and advertising layers within a wider, multi-platform ecosystem.

3.2 Language and Regional Forums

Language is one of the main organizing factors within cybercriminal forums. It influences trust, membership, target selection, criminal specialization, and access to local knowledge. However, language should not be treated as proof of nationality or location. Russian-speaking forums, for example, may include actors from Russia, Ukraine, Belarus, Moldova, the Caucasus, Central Asia, and diaspora communities (Figures 16 and 17). The apparent size of each linguistic ecosystem also depends heavily on the collection methods used. Russian- and English-language communities are often well represented in forum repositories, while Arabic-, Chinese-, French- or Latin American activity may be dispersed across Telegram, encrypted messaging applications, private groups, and temporary marketplaces. Forum statistics should therefore be interpreted as indicators of visibility rather than exact measurements of criminal activity.

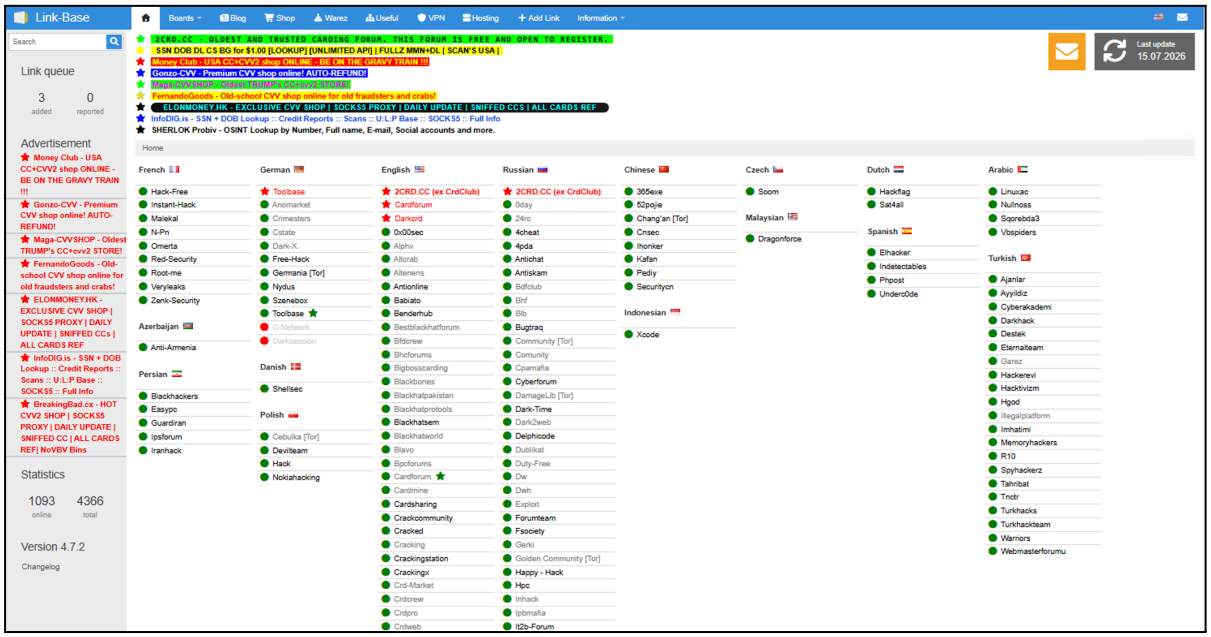


Figure 16 - Link Base worldwide cybercriminal forums repository

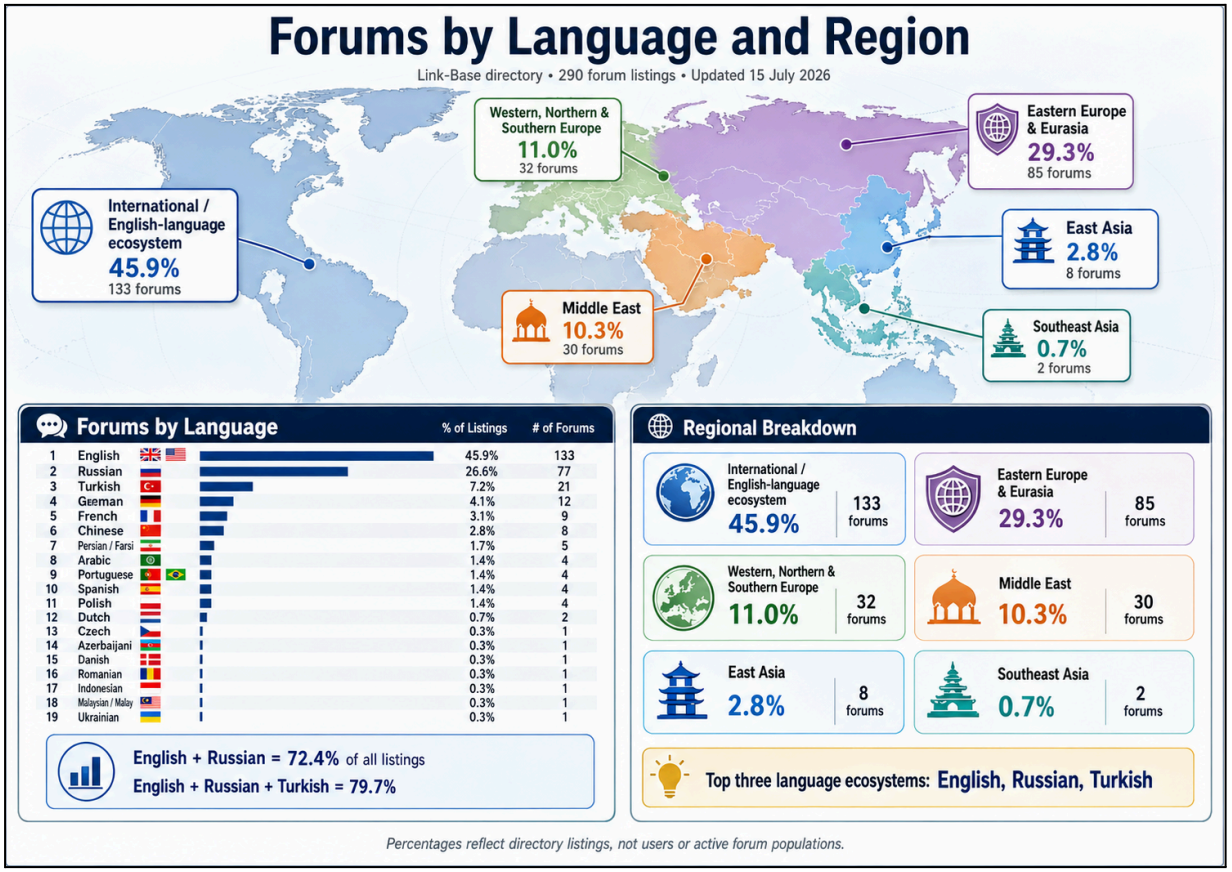


Figure 17 - Cybercrime forums statistics by languages and regions (Source: Link-based forums repository)

3.2.1 Russian-Language and Eastern European Forums

Within the wider cybercriminal forum ecosystem, Russian-language platforms and their associated Eastern European criminal communities represent one of the most mature, technically capable, and influential segments of the global underground. Although cybercriminal forums operate across multiple languages and regions, Russian-language communities have historically played a disproportionate role in developing the professional structures, specialized services, and trust mechanisms that underpin modern cybercrime. They are particularly important in malware development, ransomware, initial-access brokerage, botnets, stolen credentials, bulletproof hosting, money laundering, and other specialized attack services that are subsequently traded, resold, or operationalized across the broader international ecosystem. At the centre of this Russian-language environment are Exploit.in and XSS (Figures 18 and 19), which have remained among its most prominent, stable, and respected forums over the past decade.

These platforms constitute the core of the Russian-language forum landscape and have evolved into enduring institutions within the wider cybercriminal economy. More than discussion boards or marketplaces, they provide governance, continuity, reputation systems, dispute resolution, and trusted environments through which actors can form partnerships and conduct high-value transactions. Their structured mechanisms including reputation scores, escrow services, arbitration, vendor deposits, and invitation-only sections have influenced the operating standards of other criminal platforms. Long-standing accounts and verified transaction histories function as substitutes for legal contracts, allowing geographically dispersed and often anonymous actors to cooperate with a degree of confidence. As a result, Russian-language forums serve not only as regional criminal communities but also as central nodes connecting malware developers, access brokers, ransomware affiliates, infrastructure providers, financial specialists, and buyers from across the global cybercriminal ecosystem.

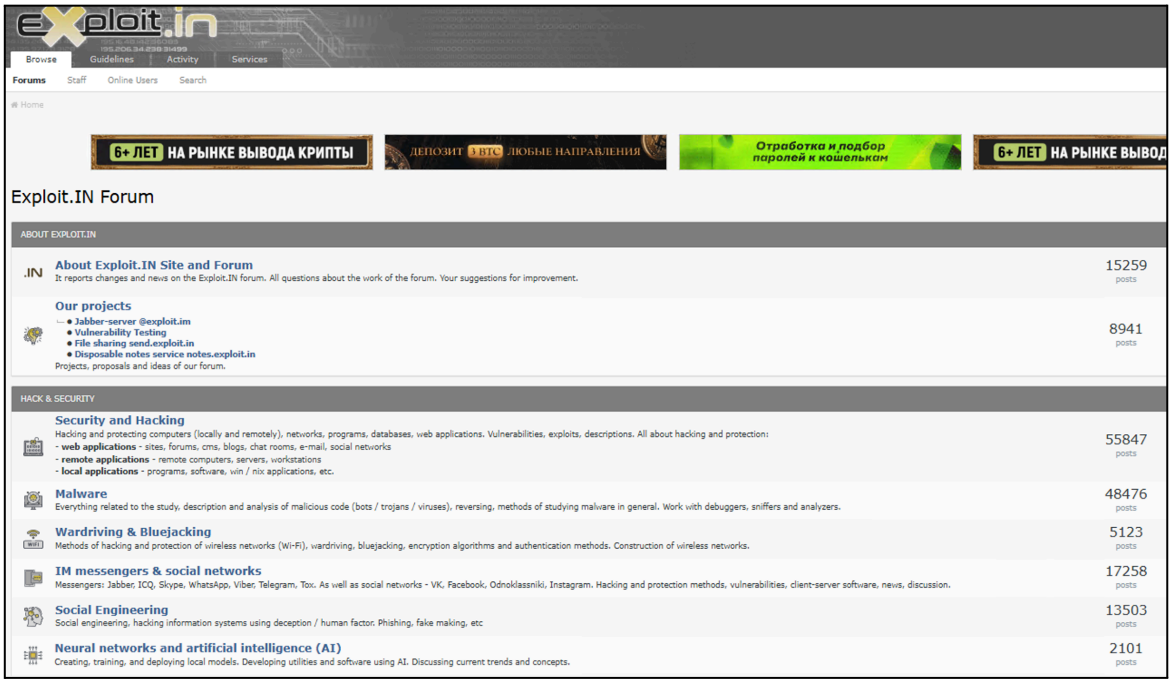


Figure 18 - An established Russian-language cybercriminal forum (source: Exploit.in)

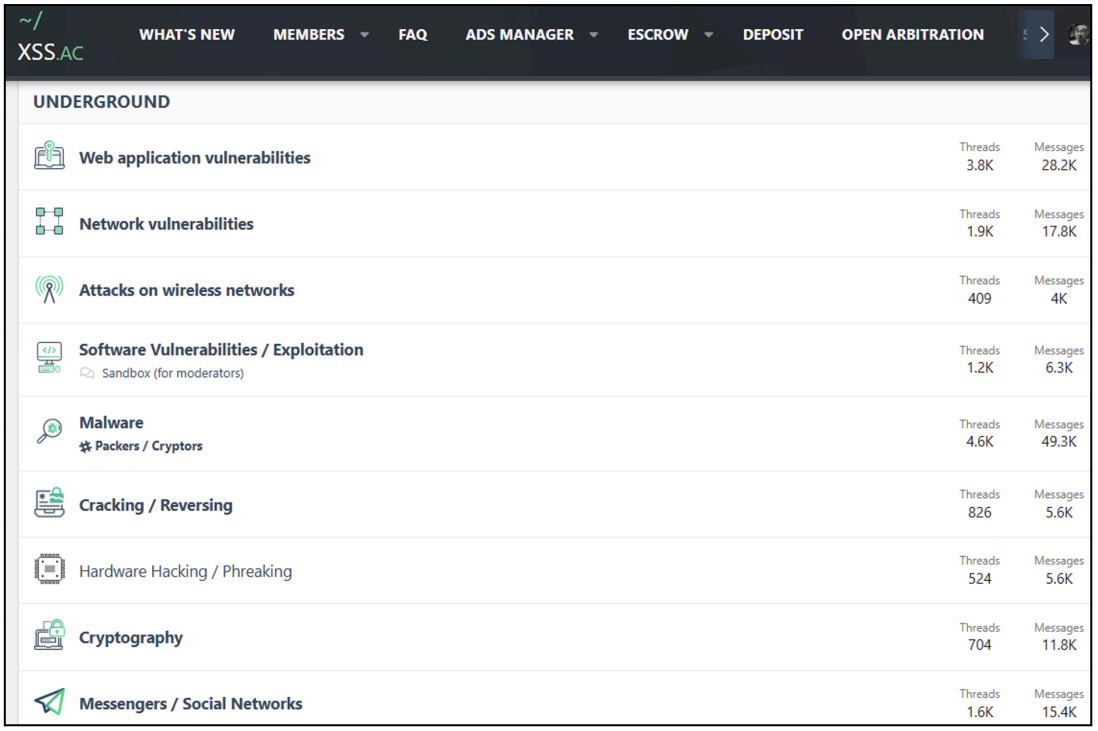


Figure 19 – An established technically oriented cybercriminal forum (source: XSS forum)

Ukrainian, Belarusian, Romanian, and other Eastern European actors may operate within Russian-language forums while also using local languages in trusted networks (Figure 20). Romanian-speaking criminal communities have historically been associated with carding, phishing, payment fraud, identity crime, and social engineering. Eastern European actors frequently switch between local languages, Russian and English, depending on whether they are recruiting trusted partners, purchasing advanced services or targeting international customers.



Figure 20 - A Romanian hacking forum (Source: Romanian Security Team forum)

3.2.2 English-Language Forums

English is the main global language of cybercriminal commerce. English-language forums bring together actors from Europe, North America, Asia, Africa, the Middle East, and Latin America and act as bridges between otherwise separate regional communities. These platforms are widely used for selling breached databases, credentials, compromised accounts, malware, phishing kits, and network access. Their accessibility attracts both experienced criminals and newcomers, but also creates greater exposure to scammers, researchers, and law enforcement. As a result, English-language forums are often unstable, with communities frequently migrating after seizures, internal disputes, or exit scams. English-language forums should not be understood as primarily British or American. English functions as the commercial lingua franca of the global cybercriminal economy (Figure 21).

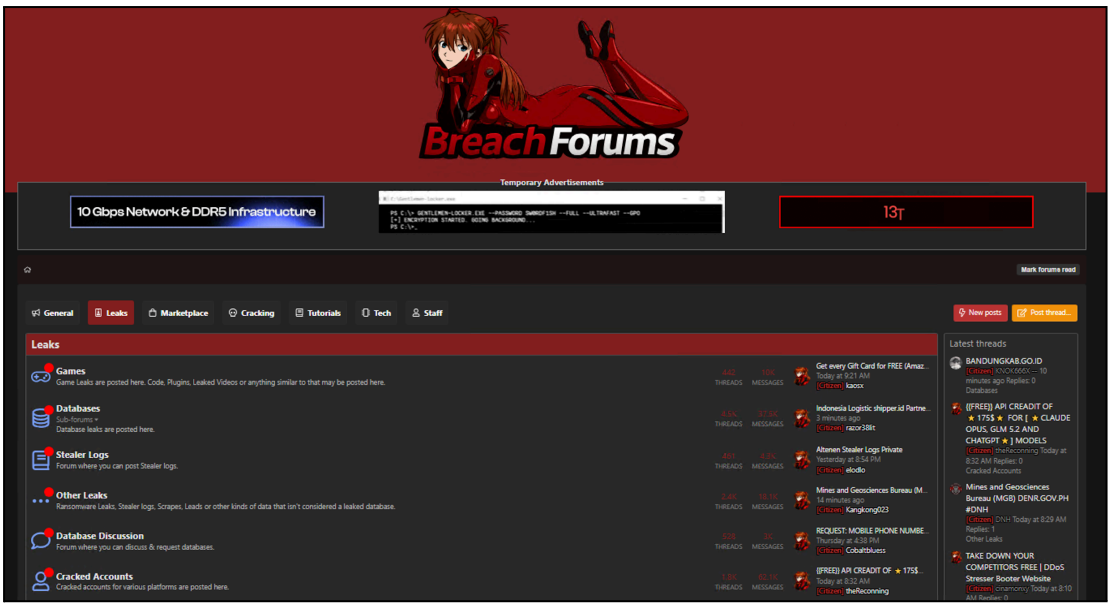


Figure 21 - An English-language cybercriminal forum specializing in stealer logs and leaked data

3.2.3 Spanish and Portuguese-Language Forums

Spanish-speaking cybercriminal communities operate across Spain, Mexico, Central America, and South America (Figure 22). Common activities include phishing, banking fraud, credential theft, account takeover, remote-access malware, SIM-related fraud, and the sale of locally targeted personal or financial data. Their main advantage is detailed knowledge of regional banks, telecommunications providers, identity systems, and payment procedures. Although the same language can support operations across several countries, successful campaigns usually require adaptation to local terminology and authentication processes.



Figure 22 - A Spanish-speaking hacking forum (Source: forum)

Portuguese-speaking activity is dominated by the Brazilian ecosystem, which has developed strong capabilities in banking Trojans, mobile malware, phishing, and payment fraud. Brazilian criminal tools are frequently designed specifically for domestic banks, digital-payment platforms, and identity systems. Significant activity also occurs through messaging applications and social-media communities rather than exclusively through traditional forums (Figure 23).

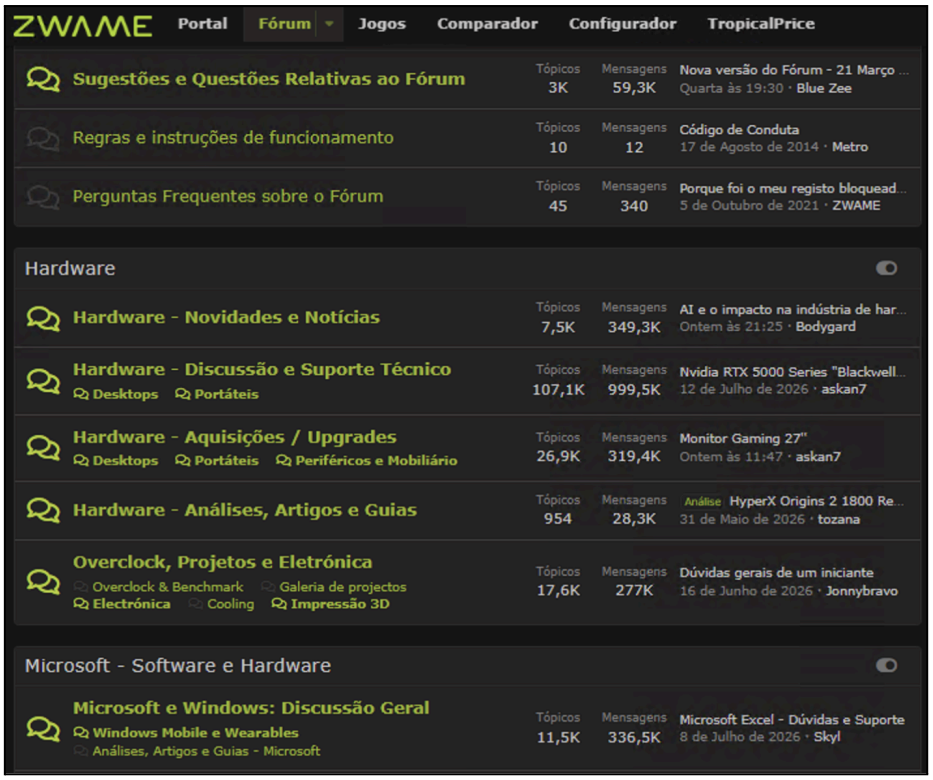


Figure 23 - A Portuguese-language technology forum containing hacking-related discussions (source: ZWAME)

3.2.4 French-Language Forums

French-speaking communities are smaller and more fragmented, but remain relevant across France, Belgium, Switzerland, Canada, and Francophone Africa. Common activities include carding, phishing, account takeover, identity-document fraud, telecommunications fraud, and the sale of stolen credentials (Figure 24). More advanced French-speaking actors often use English- or Russian-language forums to obtain malware, infrastructure, and international customers. Local French-language groups tend to rely heavily on personal trust, private channels, and small communities, partly because of persistent concerns about law-enforcement infiltration. Francophone European and African ecosystems should not be treated as identical. European actors frequently focus on banking, e-commerce, and telecommunications fraud, while some Francophone African groups are more active in business email compromise, social engineering, payment diversion, and mule recruitment.

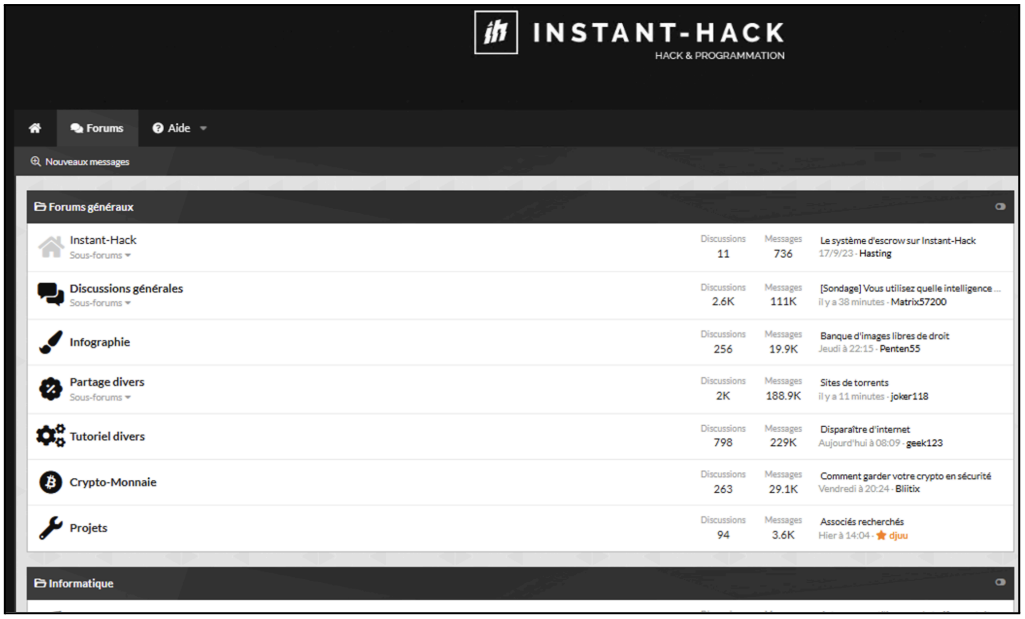


Figure 24 - A French speaking hacking forum (Source: forum)

3.2.5 Arabic and Middle East-Language Forums

Arabic-language cybercriminal communities include participants based across North Africa, the Middle East, and diaspora populations. Commonly observed activities include phishing, payment card fraud, credential theft, social media account compromise, malware distribution, website intrusion, and distributed denial-of-service attacks. The ecosystem is highly fragmented and often operates through Telegram and private messaging groups rather than large, permanent forums. Arabic-language environments may also combine financially motivated cybercrime with hacktivism, political messaging, or state-aligned activity. Analysts must therefore distinguish actors by their behavior, victim status, and monetization methods rather than by their declared ideology alone (Figures 25 and 26).



Figure 25 – An Arabic-language hacking forum (source: VBSpiders)

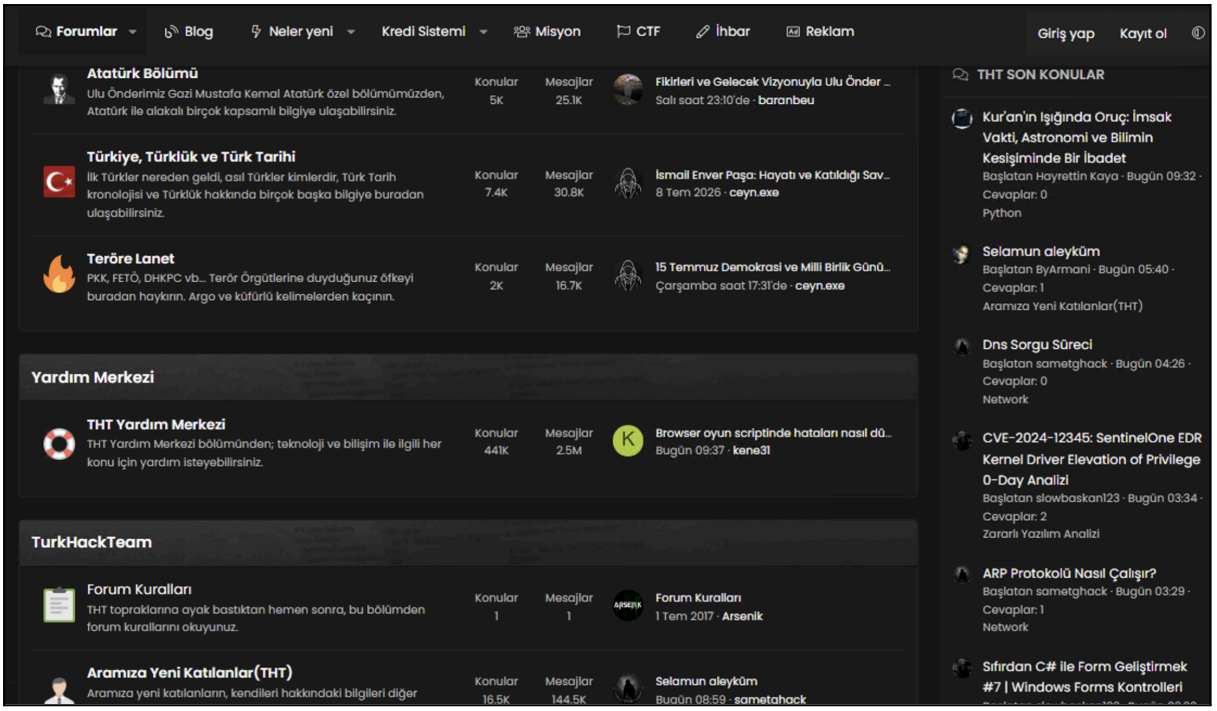


Figure 26 - A popular Turkish hacking forum (Source: Turk Hack Team)

3.2.6 Chinese-Language Forums

Chinese-speaking cybercriminal communities are less visible in Western monitoring but remain operationally significant. Their limited visibility is partly caused by the use of domestic platforms, closed messaging groups, and private broker networks. Common activities include the sale of personal data, telecommunications fraud, mobile malware, account theft, gaming-related crime, payment fraud, botnets, and money-laundering services. These markets are often closely aligned with Chinese social media, e-commerce, and digital payment ecosystems (Figure 27).

Chinese-language criminal networks are also connected to the wider East and Southeast Asian fraud economy, including underground banking, cryptocurrency laundering, and industrial-scale scam operations. However, Chinese-language cybercrime should not automatically be associated with Chinese state-sponsored activity; attribution requires additional technical and behavioral evidence.



Figure 27 - A Chinese hacking forum (Source: 365exe forum)

3.2.7 Cross-Language Criminal Activity

Cybercriminal ecosystems are increasingly interconnected. A malware developer may advertise in Russian, an access broker may sell in English, a phishing operator may work in Spanish or Arabic, and a laundering network may communicate in Romanian, Portuguese, or Chinese. Automated translation and generative artificial intelligence are reducing linguistic barriers and allowing actors to advertise, negotiate, and conduct phishing campaigns in languages they do not speak fluently. Language remains an important intelligence indicator, but it must be combined with technical evidence, payment infrastructure, victim geography, posting behavior, and cross-platform identities. For intelligence purposes, linguistic ecosystems should therefore be viewed as overlapping criminal markets rather than isolated national communities. Their significance depends not only on the number of visible forums but also on their technical maturity, trust levels, regional access, and position within the wider cybercriminal supply chain.

3.3 Network Access, Compromised Accounts, and Data Leaks forums

Forums dedicated to network access, compromised accounts, and stolen datasets occupy a strategically important position within the cybercriminal ecosystem. Rather than functioning only as repositories for leaked information, they act as brokerage and coordination environments where initial access brokers, credential sellers, and data vendors connect with ransomware affiliates, extortion groups, fraud operators, espionage-oriented actors, and other criminals seeking to monetize compromised organizations (Figure 28). Listings commonly advertise access by victim sector, geography, revenue, privilege level, and security posture, while reputation systems, escrow services, and administrator verification help reduce uncertainty between buyers and sellers. Through these forums, stolen credentials and datasets are repeatedly repackaged, resold, and reused, creating a continuous criminal supply chain in which a single compromise may support account takeover, financial fraud, ransomware deployment, data extortion, or further intrusion long after the initial breach.

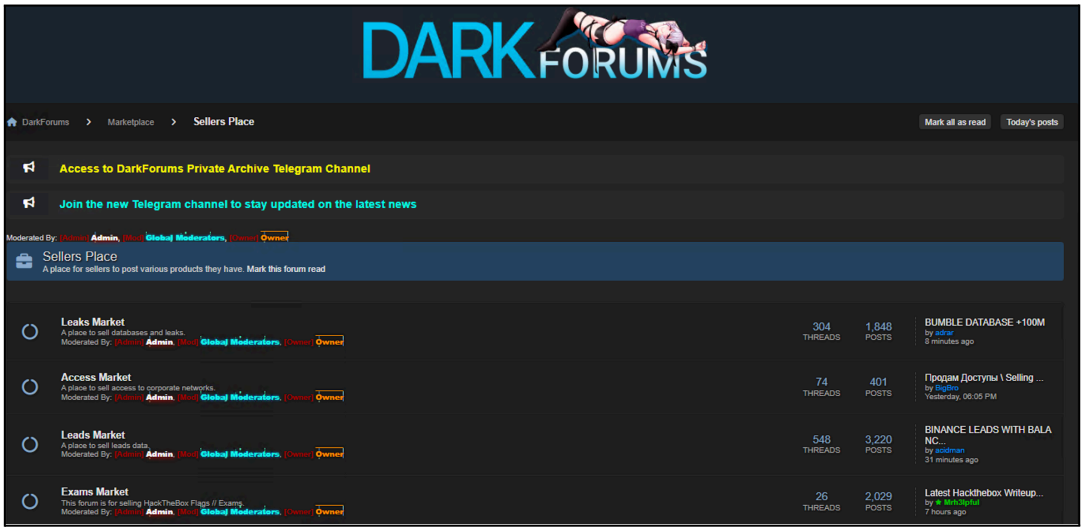


Figure 28 - A cybercriminal forum specialized in network access and data leaks

3.3.1 Initial access as a commercial product

Initial Access Brokers, or IABs, specialize in obtaining and maintaining unauthorized access to corporate environments before selling that access to other actors. The broker does not necessarily conduct the final attack. Instead, the broker identifies a vulnerable organization, establishes a foothold, verifies the level of privilege available, and advertises the opportunity to vetted buyers (Figures 29 and 30).

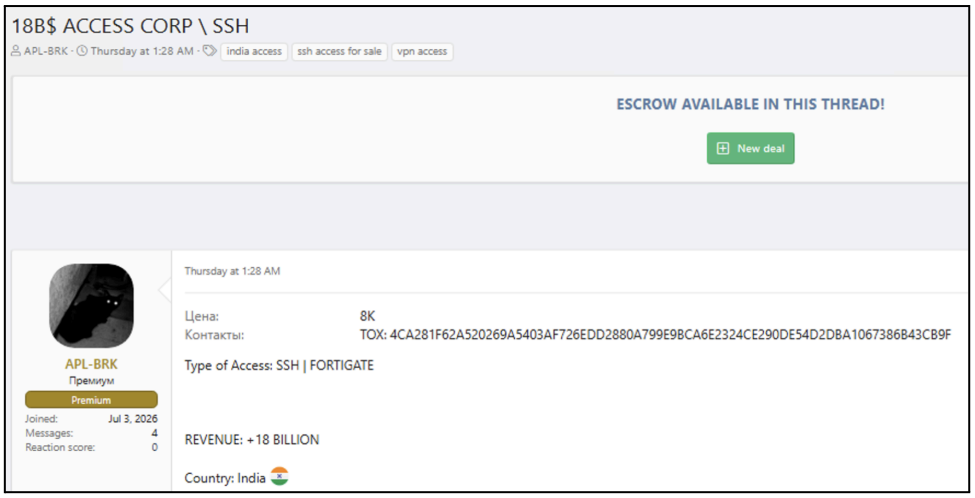


Figure 29 - Corporate SHSH access for sale on a russian cybercrime forum (Source: exploit IN forum)

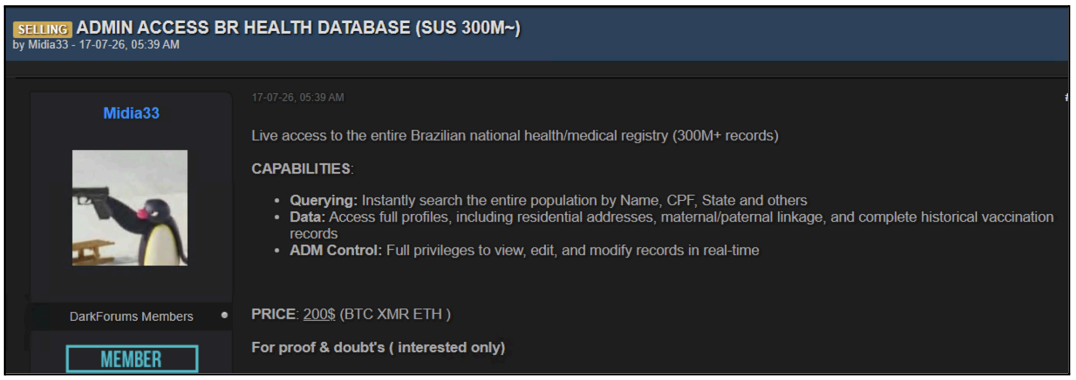


Figure 30 - Admin access to a health organization database for sale on a cybercrime forum (Source: Darkforums)

Listings commonly describe the victim without immediately disclosing its identity. Information may include:

- country and industry;
- approximate revenue or number of employees;
- type of access, such as VPN, RDP, Citrix, cloud administration, or web shell;
- user or administrator privileges;
- endpoint security products detected;
- domain structure and number of accessible hosts;
- whether backups, virtualization infrastructure, or sensitive servers are reachable.

The victim's name may only be provided privately after the buyer demonstrates funds or reputation. This protects the seller from opportunistic interference, competing criminals, and potential law-enforcement monitoring. Access is valued based on its monetization potential, not solely on the technical difficulty of obtaining it. Administrator privileges, access to identity-management systems, large revenues, cyber-insurance coverage, sensitive data, and weak segmentation increase commercial value. Conversely, access may be discounted when the organization is small, heavily monitored, already compromised by several actors, or operating in a jurisdiction considered difficult to monetize.

The relationship between access brokers and ransomware operations is particularly significant. Public advisories have documented ransomware actors obtaining access through compromised VPN or RDP credentials, exploiting externally exposed services, and recruiting brokers through criminal forums. Medusa operators, for example, have been reported to recruit IABs specifically to supply victim access, while Akira, BlackSuit, LockBit, Play, and BianLian activity has also involved the abuse of valid credentials or brokered access.

However, forum listings should not be interpreted as a complete representation of the access market. High-value transactions are often moved into private channels, Jabber servers, closed Telegram groups, or long-term broker-client relationships. Public forum posts, therefore, function partly as advertisements and as mechanisms for reputation building. The most sensitive access may never be openly listed.

3.3.2 Compromised accounts and identity-based access

A second major market concerns compromised user accounts. These range from individual consumer credentials to privileged corporate, government, financial, and cloud accounts. Common products include:

- email and webmail accounts;
- VPN and remote-access credentials;
- Microsoft 365 and cloud-platform accounts;
- banking, payment, and cryptocurrency accounts;
- e-commerce and loyalty accounts;
- social-media, advertising, and business-management accounts;
- developer, hosting, and domain-management accounts;
- accounts containing active session cookies or authentication tokens.

The criminal value of an account depends on what it enables. A corporate mailbox may support business email compromise, internal reconnaissance or password-reset interception. A cloud-administrator account can expose infrastructure and stored data. An advertising account can be used to distribute scams, while a cryptocurrency account may enable direct theft or laundering.

Modern listings increasingly offer more than a username and password. Malware logs may contain browser cookies, device fingerprints, autofill data, cryptocurrency-wallet information, and session tokens. These artifacts can allow attackers to inherit an authenticated session or reproduce aspects of the victim's device environment, potentially reducing the effectiveness of password changes and some authentication controls. This reflects a wider movement towards identity-driven intrusion. According to the Microsoft Digital Defense Report 2025, identity-based attacks increased by 32% during the first half of 2025, and more than 97% of the identity attacks observed by Microsoft were password-based, predominantly large-scale password-guessing attempts. Microsoft further reported that credentials used in such attacks were frequently obtained from credential leaks and information-stealing malware. These findings demonstrate the continuing operational value of stolen, weak, and reused credentials, while also highlighting the growing importance of session tokens and other authentication artifacts.

3.3.3 Data leaks as raw material and strategic leverage

Data-leak sections contain a mixture of newly stolen material, historical breaches, aggregated databases, and falsely advertised datasets. Typical content includes customer databases, employee records, authentication data, source code, internal documents, financial information, and personally identifiable information. The market generally distinguishes between:

- exclusive data, allegedly offered to one buyer;
- limited distribution, sold to a restricted number of customers;
- private sales, for which samples are posted but the full dataset is negotiated privately;
- public releases, shared freely to build a reputation or punish a victim;
- repackaged collections, combining older breaches or credential lists;
- stealer logs, containing information harvested directly from infected devices.

The commercial lifespan of stolen data can be considerably longer than the period immediately following a breach. The same dataset may first be sold privately, later divided by geography or record type, resold to fraud specialists, merged into larger collections, and ultimately released publicly. Different actors extract different forms of value from the same information. Corporate data may enable extortion, competitive intelligence, supplier targeting or identification of privileged employees. Personal information can support identity theft, account recovery abuse and social engineering. Credentials can be tested against unrelated services.

Telephone numbers and email addresses can feed phishing and impersonation operations. A critical analytical challenge is determining whether an advertised leak is authentic, up to date, and exclusive. Sellers frequently inflate record counts, misrepresent old databases as new breaches, recycle public information or combine legitimate samples with fabricated claims. Reliable assessment requires examination of sample consistency, timestamps, organizational structure, field names, credential validity, internal identifiers, and overlap with previously exposed material.

Intelligence implications

The most valuable intelligence is often found not in the dataset itself but in the surrounding discussion. Seller terminology, response times, preferred escrow services, relationships with ransomware affiliates, and patterns of repeated access can reveal where an actor sits in the criminal supply chain. An access listing may provide early warning of an intrusion before ransomware deployment or public disclosure. Repeated listings involving a particular technology, service provider or geography may indicate a scalable exploitation campaign. Similarly, the appearance of several organisations sharing a supplier can point to a third-party compromise rather than unrelated incidents.

Analysts should therefore treat access and leak sections as indicators of criminal intent and opportunity, while avoiding the assumption that every listing represents a verified breach. The strongest assessments combine forum monitoring with credential validation, infrastructure analysis, malware telemetry, victimology and historical actor behavior.

3.4 Carding, Financial Fraud, and Identity Crime

Carding and financial-fraud forums constitute a mature and highly specialized segment of the cybercriminal economy, providing structured environments for the acquisition, verification, sale, and monetization of stolen financial and identity data. While compromised payment cards remain a core commodity, these forums increasingly support a wider fraud ecosystem encompassing bank-account takeover, synthetic identities, fraudulent loans, cryptocurrency theft, refund abuse, mobile-payment fraud, and money-laundering services. Vendors commonly differentiate their products by geography, account balance, card type, verification status, supporting identity documents, and the level of access provided, while reputation systems, escrow mechanisms, and user reviews help establish trust and assess the reliability of illicit services. These communities therefore function not only as marketplaces, but also as knowledge-sharing and operational coordination hubs where fraud methods, bypass techniques, cash-out procedures, and laundering channels are exchanged and refined (Figure 31).

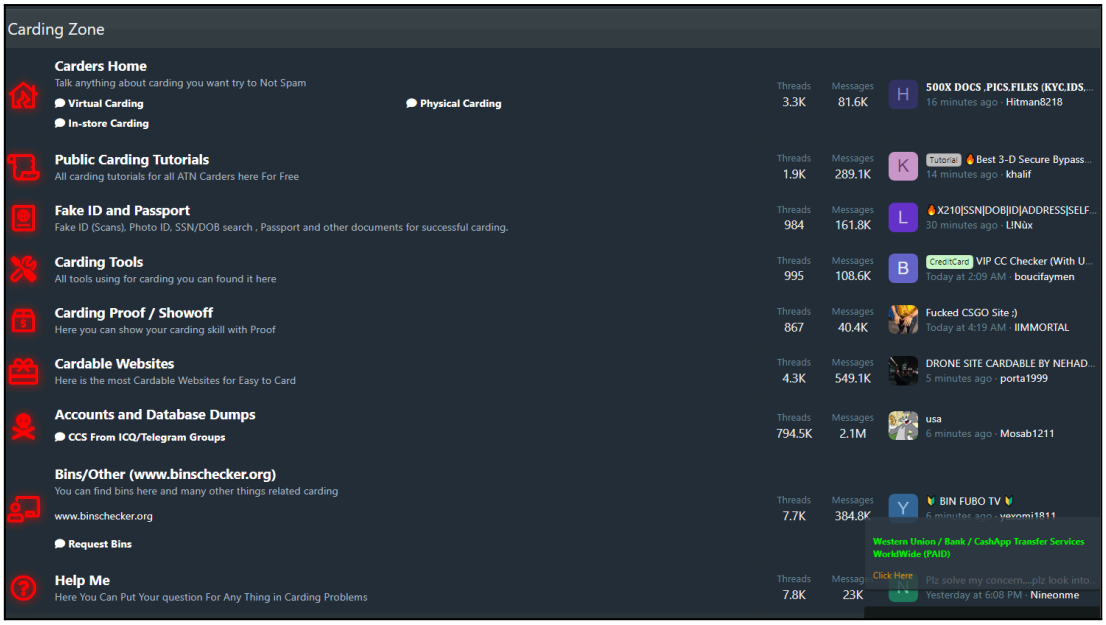


Figure 31 - A well-known English-speaking carding forum (Source: Altenen carding forum)

3.4.1 The fraud supply chain

Financial fraud is rarely carried out by a single actor from start to finish. Forums allow specialists to participate in separate stages of the operation:

- Data thieves obtain payment information or credentials through phishing, malware, skimming, social engineering or database compromise.
- Vendors validate, categorize, and advertise the stolen information.
- Buyers test the data and use it for online purchases, account takeover or cash withdrawal.
- Specialists provide fraudulent documents, mule accounts, SIM cards, drop addresses, and payment-processing assistance.
- Cash-out operators convert the stolen value into goods, cash or cryptocurrency.
- Money launderers obscure the criminal proceeds.

This division of labor lowers the technical threshold for participation. A fraud operator may purchase payment-card data, an identity profile, a proxy matching the victim's location, and access to a mule account from different vendors without personally compromising any victim. Law-enforcement actions illustrate the scale and persistence of these markets. The Rescator ecosystem allegedly advertised data connected to tens of millions of payment cards and personal records, while the BidenCash marketplace distributed millions of stolen cards as promotional material. WWH Club and associated platforms combined marketplaces, forums and training services for stolen identities, payment information, bank accounts and computer credentials.

3.4.2 Products sold in carding communities

Payment-card listings are commonly divided into several product types:

- CVV records, containing card number, expiry date, and security code for card-not-present fraud;
- fullz, combining payment-card information with the victim's name, address, date of birth, telephone number, and other personally identifiable information;
- dumps, containing magnetic-stripe track data historically used to clone physical cards;
- bank logs, providing access to online banking accounts;
- merchant or payment-processor accounts, used to process unauthorized transactions;
- verified cryptocurrency or financial accounts, sometimes accompanied by identity documents;
- identity packages, containing sufficient information to impersonate a person or establish fraudulent accounts.

Pricing reflects the probability that the information remains valid and monetizable. Relevant factors include issuing country, bank, card type, balance or credit limit, age of the data, and the availability of supporting identity information. Fresh, geographically targeted, and verified records command a premium. Heavily circulated or poorly validated data are sold at lower prices in bulk. The advertised price should not be confused with the eventual financial loss. Stolen data is discounted because buyers assume operational risk: cards may already be canceled, transactions may be blocked, the vendor may be fraudulent, or cash-out attempts may expose the buyer.

3.4.3 Identity crime beyond payment cards

The growing emphasis on complete identity profiles reflects the expansion of fraud into services that rely on digital onboarding. Criminals seek identity documents, selfies, proof-of-address records, tax information, telephone numbers and access to email or mobile accounts. These materials support:

- fraudulent bank and cryptocurrency accounts;
- credit and loan applications;
- government-benefit fraud;
- tax-refund fraud;
- insurance and healthcare fraud;
- mobile-number takeover;
- account-recovery manipulation;
- creation of mule or shell identities.

Identity packages can be reused across several schemes. A profile may initially be used to open an account, later sold as a verified account, and eventually reused for social engineering against the original victim. The result is a circular economy in which personal information, accounts, and fraud-enabling services are repeatedly traded. Synthetic identity fraud is a particularly complex form of fraud. Actors combine genuine identity elements, such as a valid government-issued identification or credit-profile number, with fabricated names, addresses or supporting documents. These identities may be cultivated over time to establish credit histories before being used in higher-value fraud.

3.4.4 Services and operational knowledge

Fraud forums are not limited to selling data. They provide tutorials, mentoring, software, and operational services. Discussions may cover fraud-detection systems, transaction limits, merchant behavior, document requirements, and regional banking practices. Specialized vendors may offer:

- phishing pages and banking panels;
- one-time-password interception;
- counterfeit identity documents;
- residential proxies and anti-detect browsers;
- fraudulent invoices and proof-of-funds documents;
- money-mule recruitment;
- parcel redirection and reshipping;
- account verification;
- laundering and cryptocurrency conversion.

Some communities operate as informal training centers where inexperienced members purchase courses or “methods.” The quality varies considerably. Established fraud techniques coexist with copied tutorials, obsolete procedures, and deliberate misinformation designed to attract inexperienced buyers.

3.4.5 Trust, deception and market instability

Fraud communities are characterized by extensive internal fraud. Vendors may sell invalid cards, fabricated balances, publicly available records, or accounts that they later recover. Buyers may falsely claim that the data was invalid to demand refunds. Administrators and guarantors attempt to control these disputes through escrow, deposits, arbitration, and reputation systems. Vendor status is, therefore, an important commercial asset. Successful sellers publish customer reviews, transaction proofs, and replacement rate statistics. Some provide limited guarantees when cards or accounts fail within a specified period. Others maintain private shops outside the forum once they have accumulated sufficient customers. The takedown of major marketplaces does not eliminate the underlying economy.

Sellers migrate to replacement forums, private channels or independent shops, while leaked databases and vendor contacts survive the closure. In June 2025, US authorities seized approximately 145 clear-web and darknet domains, together with cryptocurrency funds, associated with the BidenCash marketplace. According to the US Department of Justice, the marketplace had more than 117,000 customers, facilitated the trafficking of more than 15 million payment-card records and associated personal information, and generated more than US$17 million during its operation. The action demonstrates both the scale of the marketplace and the distributed infrastructure required to support such criminal services.

Intelligence implications

Analysis should focus on the entire fraud-enabling chain rather than only counting card listings. A sudden increase in data from one issuer, merchant or region may indicate an active compromise. New cash-out instructions may reveal changes in payment controls. Demand for accounts on a particular platform may reveal that a service is being exploited before the resulting fraud is widely reported.

Cross-referencing vendor identities, cryptocurrency addresses, communication handles and product samples can reveal links between data thieves, fraud operators and laundering services. Nevertheless, forum claims require caution. Sales volumes, account balances and success rates are routinely exaggerated, and the most capable fraud networks may operate largely outside public discussions.

3.5 Hacking, Malware, and Cyberattack Services

Forums specializing in hacking, malware, and cyberattack services form an important technical marketplace within the wider cybercriminal ecosystem (Figure X). They enable threat actors to acquire offensive tools, infrastructure, and expertise without having to develop malware, discover vulnerabilities or construct attack capabilities independently. Products and services advertised through these communities may include Remote-Access Trojans, information stealers, ransomware builders, exploits, web shells, phishing kits, loaders, botnets, crypters, credential-testing tools, and distributed denial-of-service capabilities. Vendors may also provide command-and-control servers, bulletproof hosting, proxy networks, virtual private servers, domain infrastructure, and other resources required to deploy, conceal, and sustain malicious operations.

More advanced offerings can include exploit development, malware customization, antivirus evasion, code obfuscation, penetration of specific targets and the compromise of websites, servers, email accounts or corporate networks. Some providers offer complete attack packages or operate on a malware-as-a-service, botnet-as-a-service, or hacking-for-hire basis, allowing customers to rent capabilities, commission targeted intrusions, or outsource particular stages of an operation.

These markets lower the technical barriers to cybercrime by providing less experienced actors with ready-made, configurable, and often supported offensive capabilities. At the same time, they allow malware developers, exploit sellers, infrastructure providers, and skilled hackers to monetize specialized knowledge across a broader criminal customer base. The resulting division of labor enables actors with limited technical expertise to conduct increasingly sophisticated attacks by combining tools and services obtained from multiple specialized providers.

3.5.1 Malware products and service models

Malware is sold through several commercial models:

- one-time sale of source code or a compiled build;
- monthly or lifetime licenses;
- subscription access to a control panel;
- Malware-as-a-Service;
- affiliate programs based on revenue sharing;
- private builds customized for a specific buyer;
- rented botnets or access to already infected devices.

Frequently advertised products include information stealers, remote-access Trojans, loaders, botnets, phishing kits, cryptocurrency drainers, ransomware builders and tools designed to evade security controls. The distinction between a malware developer and an operator is important. Developers may never directly compromise a victim. Their role is to maintain the code, update evasion features, operate licensing systems, and provide customer support. Affiliates or customers handle distribution and victim selection. This separation creates resilience. When one operator is arrested, or one campaign is disrupted, the same malware family, infrastructure provider, or access source may continue serving other customers.

3.5.2 Malware-as-a-Service and affiliate structures

Service-based models have transformed technical cybercrime by reducing development requirements. Customers can access dashboards, generate customized payloads, manage infections, and receive stolen data through an interface resembling legitimate software services. Service providers may advertise:

- regular updates;
- compatibility with current operating systems;
- encryption or obfuscation;
- control-panel hosting;
- technical support;
- infection statistics;
- automated log filtering;
- integration with Telegram or other notification systems;

- Replacement of builds detected by antivirus products.

Ransomware affiliate programs represent a more controlled version of this model. Core operators maintain the malware, payment infrastructure, negotiation systems, and leak sites, while affiliates obtain access and execute attacks. Revenue is divided according to an agreed percentage. Membership is not always open. Established programs may require evidence of previous compromises, a forum deposit, recommendations from trusted actors or an interview with the operator. This limits infiltration and reduces the risk created by inexperienced affiliates.

3.5.3 Hacking-for-hire and specialized services

Forums also host actors offering intrusion services against websites, corporate networks, social-media accounts, email accounts or online infrastructure. Advertisements may use broad expressions such as “penetration testing” or “recovery services,” although the surrounding forum, payment model and absence of authorisation often indicate malicious intent. Service offerings may include:

- website compromise and defacement;
- database extraction;
- credential theft;
- account takeover;
- distributed denial-of-service attacks;
- exploitation of exposed services;
- vulnerability discovery;
- malware installation;
- data deletion or disruption;
- targeted phishing campaigns.

More sophisticated operators may avoid fixed-price public menus and instead request information about the target, objective, geography, security posture, and time constraints before providing a quotation. Targets perceived as particularly sensitive or operationally risky, including governments, critical infrastructure operators, and prominent individuals, may be refused, priced substantially higher or handled only through private referrals.

- Bulletproof hosting;
- virtual private servers;
- domains and DNS services;
- residential and mobile proxies;
- compromised servers;
- malware-signing certificates;
- traffic-distribution systems;
- crypters and obfuscation services;
- spam and SMS delivery;

- CAPTCHA-solving services;
- DDoS-for-hire infrastructure.

These services are not peripheral. They determine whether malware can be delivered, whether command-and-control infrastructure remains online, and whether criminal activity can withstand abuse reports or defensive intervention. The same provider may support several unrelated operations. Infrastructure overlaps can therefore reveal connections between actors that do not publicly interact. However, shared infrastructure can also result from customers purchasing services from a common vendor and does not automatically prove common ownership.

3.5.4 Technical claims and product quality

Malware advertisements frequently contain inflated claims such as “fully undetectable,” “zero-day,” “all antivirus bypass,” or “exclusive exploit” (Figure 32). These statements are primarily marketing language. Products may contain copied code, public exploits or backdoors inserted by the seller. Buyers commonly request demonstrations, scanning results, sample builds or escrow-based testing. Reputable sellers may restrict demonstrations to prevent theft or the creation of fraudulent signatures. Some provide updates when detection rates increase, while others abandon a product and relaunch it under a different name.

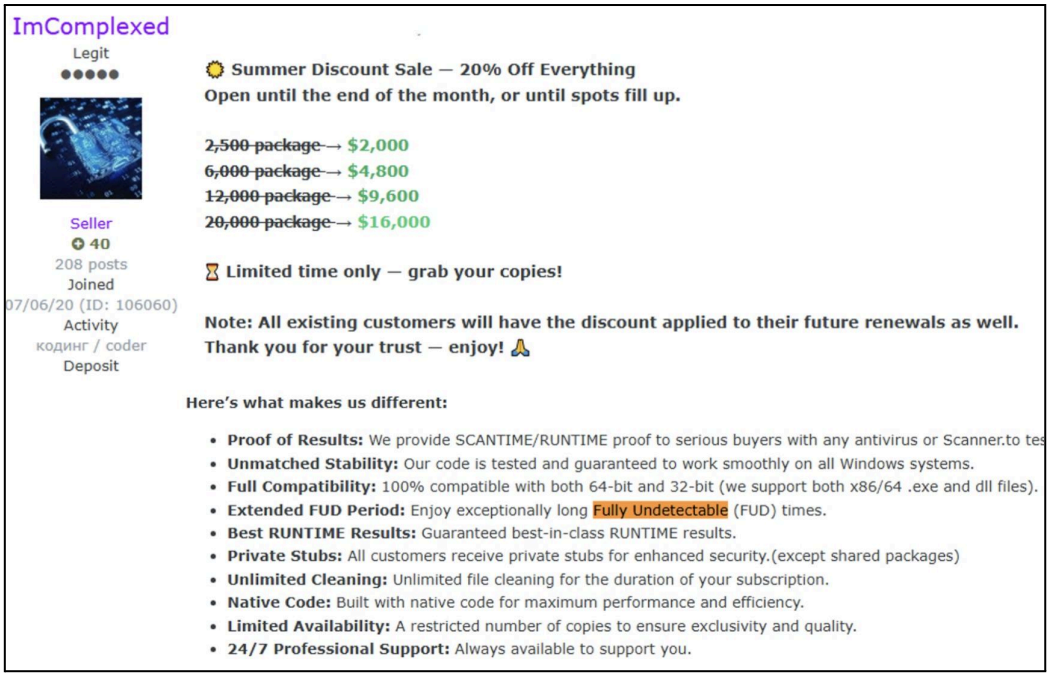


Figure 32 – Advertisement claiming to offer a private “fully undetectable” crypter (source: Exploit.in)

The developer's reputation is often more important than the advertised feature list. Long-term presence, technical support, previous releases and acceptance by established forum members provide stronger credibility indicators than screenshots or unsupported claims.

3.5.5 Forums as recruitment and coordination environments

Technical sections also facilitate recruitment. Malware developers seek distributors; ransomware operations recruit affiliates; botnet operators look for buyers; and access brokers advertise opportunities to intrusion teams. This means that forums should be analyzed as coordination environments rather than simply online shops. Public posts may initiate relationships that later migrate to private messaging. Recruitment requirements can provide insight into an operation’s maturity, geographic priorities, and immediate needs. For example, demand for specialists in virtualization environments, cloud administration or particular enterprise technologies may indicate the intended direction of future attacks. Requests for access in specific countries or industries can similarly provide early indicators of targeting priorities.

Intelligence implications

The presence of a tool on a forum does not establish that it has been successfully deployed. Analysts should distinguish between advertisement, demonstrated capability, confirmed sale, and observed operational use. High-value indicators include:

- technical details consistent with malware samples;
- shared infrastructure or cryptocurrency addresses;
- Repeated interaction between developers and known operators;
- customer complaints, identifying defects or failed campaigns;
- recruitment posts linked to subsequent attacks;
- updates corresponding to changes in defensive detection;
- Vendor migration following the forum disruption.

Forum intelligence is most powerful when combined with malware analysis, infrastructure tracking, victim reporting, and financial investigation. Posts can reveal intent and commercial relationships, but technical evidence is required to establish operational attribution. Across all three categories, the central reality is the same: cybercriminal forums support a fragmented but interconnected service economy. Access brokers, malware developers, fraud specialists, data vendors, and laundering services perform different functions, allowing criminal campaigns to be assembled from independently purchased components. The analytical priority should therefore be to identify the relationships between these components rather than assess each advertisement in isolation.

4. Threat Actors and Criminal Supply Chains

Cybercriminal forums bring together actors who perform various roles in a criminal operation. One actor may steal credentials, another may sell access to a compromised organization, another may provide malware or infrastructure, and a separate specialist may conduct fraud, extortion, or money laundering. These actors do not necessarily belong to the same group. They may cooperate only for a single transaction or campaign.

The main characteristic of this ecosystem is therefore its modular structure. Criminals no longer need to possess every technical and operational capability themselves. Access, malware, infrastructure, stolen data, financial services, and specialist expertise can all be purchased or rented. This allows less capable actors to conduct more complex attacks and enables experienced criminals to expand their operations more quickly. This specialization also complicates attribution. Two attacks may use the same malware, hosting service, access broker, or laundering network, even if they are not controlled by the same organization. The common element may simply be a commercial provider serving several unrelated customers. Analysts should therefore focus not only on individual usernames or criminal brands, but also on the relationships, transactions, infrastructure, and financial connections between actors.

4.1 Main Threat Actors in the Criminal Supply Chain

Within the cybercrime and hacking forum ecosystem, several types of threat actors play recurring roles, including:

- **Initial-access brokers** obtain or purchase access to compromised organizations and sell it to other criminals. The access may involve remote desktop accounts, virtual private networks, cloud accounts, web shells, email accounts, administrative privileges, or authenticated browser sessions. These brokers are important because they connect the initial compromise of a victim with later activities such as ransomware, fraud, data theft, or espionage.
- **Malware developers and service operators** provide tools such as stealers, loaders, remote-access malware, phishing kits, botnets, and ransomware. Some sell their products directly, while others use subscription or affiliate models. Their customers may receive technical support, updates, infrastructure, and access to management panels.

- **Affiliates and intrusion operators** use the access and tools supplied by others to conduct attacks. They may perform lateral movement, privilege escalation, data theft, ransomware deployment, or extortion. In many cases, these operators are responsible for the practical execution of the attack, even though the malware, infrastructure, and access were obtained from separate providers.
- **Data brokers and fraud specialists** help convert stolen information into money. Data brokers sell databases, internal documents, credentials, personal information, and financial records. Fraud specialists use this information to detect account takeover, identity theft, payment fraud, social engineering, and other criminal activity.
- **Infrastructure providers** supply hosting, domains, proxies, servers, command-and-control systems, and malware-delivery services. Some knowingly serve criminal customers, while others operate under weak controls, through resellers, or with permissive abuse policies. The same provider may support several unrelated criminal operations.
- **Laundering services,** cash-out specialists, and money mules move and convert criminal proceeds. Their role may begin only after the attack is complete. They may have no direct involvement in the original intrusion but remain essential to the final monetization of the crime.

Some actors act as brokers or coordinators rather than supplying a single capability. They connect access sellers, malware operators, fraud specialists, infrastructure providers, and laundering networks. Their value lies in their contacts, reputation, and ability to quickly assemble the required services. The same actor may perform more than one role. An access broker may also conduct intrusions, a malware developer may operate independent campaigns, and a forum administrator may also provide escrow or brokerage services. Actor roles should therefore be assessed according to the activity observed in a particular case rather than treated as fixed identities.

4.2 From Access to Monetization

The criminal supply chain usually begins with the acquisition of credentials, access, data, or another useful asset. This may result from phishing, malware infections, vulnerability exploitation, credential reuse, scanning, social engineering, or insider activity. The initial asset may have limited value until it is validated and enriched. A seller may confirm that credentials remain active, identify the victim organization, determine the level of privilege, examine the security products in use, or identify sensitive systems and data. This additional information can significantly increase the value of the access. The asset may then be sold or transferred to another actor. Transactions can take place through public listings, private messages, encrypted communication channels, brokers, auctions, or revenue-sharing agreements.

The seller may continue to provide assistance after the sale by replacing failed credentials, maintaining persistence, or helping the buyer understand the victim environment. The buyer may use the access for different purposes. These can include data theft, business email compromise, financial fraud, cryptocurrency theft, ransomware, extortion, espionage, or the resale of access to another criminal.

The final objective is not always known at the time of the sale. An access broker may sell access without knowing whether the buyer intends to steal data, deploy ransomware, or conduct espionage. An actor may also change objectives after entering the network and discovering valuable information or systems. After the attack, the proceeds must be moved, divided, and concealed. This may involve cryptocurrency exchanges, peer-to-peer traders, money mules, informal brokers, shell companies, or professional laundering networks.

The value of the stolen asset may continue after the original attack. Credentials can be reused, internal documents can support social engineering, customer data can enable fraud, and source code can reveal further vulnerabilities. Stolen information may therefore be sold and exploited several times. The process should not be understood as a simple linear chain. The same access may be sold to multiple buyers, different actors may exploit the same victim, and stolen data may repeatedly move between forums, marketplaces, and private communication channels.

4.3 Criminal Relationships and Intelligence Value

The most valuable intelligence often appears when one threat actor transfers access, data, tools, infrastructure, or money to another. These transfers can reveal relationships that are not visible from public advertisements alone. For example, an access broker may provide credentials to an intrusion operator, a malware developer may recruit affiliates, or a criminal group may transfer stolen funds to a laundering service. Messages regarding technical support, failed access attempts, payment disputes, replacements, or escrow can provide evidence that a transaction occurred. Analysts should pay particular attention to repeated contact between actors, shared communication details, cryptocurrency addresses, infrastructure, customer feedback, and dispute records.

These indicators can help identify suppliers, customers, intermediaries, and operational dependencies. However, using the same service does not necessarily prove that two actors belong to the same group. Several criminals may purchase infrastructure, malware, or access from the same provider. Shared resources should therefore be treated as evidence of a possible connection, not as proof of common control. The main purpose of supply-chain analysis is to understand how separate criminal capabilities are combined. This approach can identify the actors who provide essential services, the relationships that connect different operations, and the points at which investigation or disruption may have the greatest effect.

5. Forum Assessment and Intelligence Collection

Cybercriminal forums generate large volumes of information, but only a small proportion has immediate intelligence value. Posts may contain recycled data, false claims, copied advertisements, deliberate deception, low-level discussion, or outdated material. Effective monitoring, therefore, depends less on collecting everything than on identifying the information that changes an assessment, reveals exposure, confirms a criminal relationship, or supports preventive, investigative, or disruptive action.

Forum intelligence should be collected against defined intelligence requirements. The objective may be to determine whether an organization has been compromised, identify actors targeting a particular sector, track the development of a malicious capability, understand the movement of stolen information, or map the services supporting a criminal operation. Without a clear purpose, analysts may collect large amounts of material while missing short-lived, operationally important activities.

Assessment should distinguish among the forum, the actor, and the individual claim. A well-established forum can contain fraudulent vendors. A reputable actor can make an inaccurate statement. A low-quality platform can occasionally contain unique and highly valuable information. Treating all three levels as equally reliable creates analytical error.

5.1 Assessing Forums, Vendors, and Listings

A forum should first be assessed as an environment. Longevity, membership size, and post volume may indicate activity, but they do not necessarily indicate criminal significance. A large platform may be dominated by copied leaks, inexperienced users, automated content, and fraudulent advertisements. A smaller platform may host a limited number of highly capable vendors and brokers.

The most important indicators are commercial depth, threat actor quality, access restrictions, evidence of completed transactions, and the forum’s connections to wider criminal networks. Disputes, escrow activity, customer feedback, private sections, vendor verification, and recurring commercial relationships generally provide more intelligence value than raw membership figures. Analysts should also examine the forum’s leadership and continuity. Administrator history, domain changes, infrastructure reuse, payment systems, disputes, security incidents, and links to previous platforms can reveal whether the forum represents an established community, a temporary replacement, an impersonation, or an exit scam.

A forum that has been seized or compromised may remain accessible for a period. Continued availability does not prove that criminal administrators still control the platform. Changes in moderation behavior, unusual administrator messages, sudden payment requests, or altered communication channels may indicate law-enforcement control, internal compromise, or fraudulent succession. Vendor assessment should focus on identity continuity and demonstrated capability. Usernames alone are weak identifiers because they can be changed, sold, stolen, copied, or deliberately impersonated. Analysts should compare contact handles, cryptocurrency addresses, encryption keys, language patterns, working hours, infrastructure, profile images, previous advertisements, and relationships with known actors.

Reputation scores should not be accepted at face value. Positive reviews may be fabricated, reciprocal, purchased, or based on low-value transactions. More reliable indicators include repeat customers, technically credible samples, consistent delivery over time, successful dispute outcomes, and external evidence linking the vendor to genuine criminal activity. Negative information can be particularly valuable. Complaints and disputes may reveal payment details, private conversations, technical failures, product samples, victim information, and hidden relationships. A vendor’s response to criticism may also reveal whether the actor controls the advertised product or is merely reselling material obtained elsewhere.

Individual listings should be assessed for recency, originality, specificity, technical plausibility, and supporting evidence. A detailed listing is not automatically credible, but vague claims without verifiable information should be treated cautiously. The analyst should determine whether the material is original or copied from another platform. Recycled databases, repackaged malware, and repeated access advertisements are common. An old dataset may still have value for identity resolution or social engineering, but it should not be presented as evidence of a current compromise unless additional information confirms continued relevance.

The strongest validation comes from independent evidence. This may include internal security telemetry, victim reporting, infrastructure activity, malware analysis, financial tracing, or later operational use. Analysts should clearly distinguish between access being advertised, access being validated, a sale being claimed, and access being used in an attack. Confidence should reflect both the reliability of the source and the credibility of the information. High confidence normally requires several independent indicators or direct technical, financial, or victim-side confirmation. Moderate confidence may be appropriate when the source has a credible history and the claim is plausible but not independently verified. Low confidence should be used where the source is unknown, the claim is inconsistent, or the available evidence may be promotional or deceptive.

An assessment should also state what remains unknown. It may be possible to confirm that credentials were offered for sale without verifying their validity. A vendor may claim that access was sold without identifying the buyer. A malware service may be advertised without evidence that it has been successfully deployed. Expressing these limits makes the intelligence more useful and defensible.

5.2 Monitoring Methods and Collection Priorities

Monitoring should begin with a clear set of intelligence questions. These questions may concern a specific organization, sector, technology, threat actor, criminal service, or geographical area. Collection priorities should reflect the potential impact of the activity and the likelihood that forum intelligence can provide early warning or investigative value. Organization-focused monitoring should include brand names, domains, subsidiaries, executive names, email domains, products, internal terminology, and common misspellings. Criminal actors frequently shorten names, use local-language variants, remove punctuation, or refer to victims indirectly. Monitoring should therefore account for transliteration, abbreviations, code words, and contextual references.

Actor-focused monitoring requires a longer-term approach. Analysts should maintain timelines of observed identities, services, contacts, payment information, infrastructure, disputes, forum migrations, and relationships with other actors. This can reveal changes in role, capability, customer base, or operational pressure. An actor may disappear from one forum and reappear under a different name or on another platform. Continuity may be indicated by reused contact details, writing style, cryptocurrency addresses, encryption keys, infrastructure, pricing, or relationships with the same customers and guarantors. Event-driven monitoring is also important. The collection should intensify following major vulnerability disclosures, significant data breaches, arrests, sanctions, malware disruptions, forum seizures, ransomware takedowns, or geopolitical crises. These events often lead to migration, impersonation, emergency recruitment, infrastructure replacement, and changes in criminal demand.

Forum disruption provides a particularly valuable monitoring opportunity. After a takedown, analysts should track successor platforms, false replacement sites, authentication methods used by administrators, vendor migrations, and changes in trust relationships. The movement of established actors may reveal the true continuity of the criminal community more clearly than the survival of the original domain. Automation can support collection, but it should not replace analyst judgment. Automated tools can assist with translation, deduplication, entity extraction, keyword alerting, and trend identification.

However, they may misinterpret criminal slang, sarcasm, coded language, reposted content, and deliberately misleading claims. Manual review remains essential where context determines meaning. A phrase that appears to describe a sale may actually be a scam accusation, a joke, a quotation from another forum, or an attempt to damage a competitor. Automated systems may also fail to distinguish between an original listing and a copy of an advertisement. The collection should preserve context. The value of a post often depends on the surrounding discussion, the actor's history, replies from other users, and subsequent changes. Analysts should record the date, platform, section, username, content, supporting images, links, contact information, and relevant responses. Short-lived content should be preserved promptly where collection is lawful and authorized. Posts may be edited or deleted, accounts may be banned, and forums may disappear without warning. However, the desire to preserve evidence should not override legal restrictions, handling requirements, or researcher safety.

Cross-platform collection is increasingly necessary because higher-value activity often moves away from public forums. A listing may appear on a forum, while negotiation, delivery, and payment occur through Telegram, Jabber, TOX, private chat groups, or encrypted messaging. Forum monitoring should therefore be combined with infrastructure analysis, financial intelligence, malware analysis, and broader open-source research. Collection priorities should favor activity that indicates direct exposure or operational intent. Current access listings, active credentials, recruitment for specialized capabilities, victim-specific data, and requests targeting a particular technology or sector generally deserve higher priority than generic discussion or historical leaks. The objective is not to maintain the largest archive. It is to identify the information that provides a warning, explains relationships, supports attribution, or creates an opportunity for intervention.

5.3 Researcher Security, Legal, and Ethical Considerations

Research into cybercriminal forums involves legal, operational, and ethical risks. The fact that information is technically accessible does not automatically mean that every collection method is authorized or appropriate. Passive observation of publicly available material is different from entering restricted communities under false pretenses, communicating directly with criminals, purchasing illegal goods, downloading stolen data, or participating in transactions. Organizations should define clearly what researchers are permitted to access, collect, retain, and share.

Researchers should avoid actions that could be interpreted as encouraging criminal activity, facilitating a transaction, or creating demand for illegal services. Direct engagement with threat actors may also expose the researcher or organization to manipulation, targeting, blackmail, or legal scrutiny.

The handling of stolen personal information requires particular caution. Data may contain credentials, financial records, health information, identity documents, or information concerning vulnerable individuals. Collection should be limited to what is necessary for the intelligence purpose, and access should be restricted to authorized personnel.

Researchers should not retain large volumes of stolen data simply because it is available. In many cases, metadata, screenshots, hashes, sample records, or limited indicators may be sufficient to establish relevance without storing the full dataset. Operational security should include separation between research environments and the rest of the organization. Researchers should use controlled infrastructure, appropriate identity protection, secure storage, logging, and malware-handling procedures. Files obtained from criminal platforms should be treated as potentially malicious.

Forum access can also expose researchers to phishing, malware, tracking, social engineering, and attempts to identify their real identity. Criminal actors may place malicious documents, links, or software within advertisements and private messages. Researchers should assume that the environment is hostile and that apparently routine interactions may be attempts to compromise them.

Legal considerations vary across jurisdictions. Relevant issues may include unauthorized access, interception, possession of stolen data, controlled material, privacy law, sanctions, evidence handling, and contact with designated organizations. Legal review should be integrated into collection planning rather than sought only after a problem occurs. Ethical analysis should consider proportionality and necessity. The potential intelligence value of obtaining additional information should be balanced against the risk of harming victims, exposing personal data, interfering with an investigation, or strengthening a criminal market.

Researchers should also consider deconfliction. A forum, actor, or transaction may already be subject to a law-enforcement or intelligence operation. Uncoordinated engagement may alert the target, disrupt evidence collection, or create risks for another investigation. The safest and most defensible approach is to establish written collection authorities, clear escalation procedures, data-handling rules, and regular legal and security review.

6. Turning Forum Activity into Actionable Intelligence

Forum monitoring becomes valuable when information is converted into an assessment that supports a decision. Raw posts, screenshots, usernames, and advertisements are not actionable intelligence by themselves. They must be interpreted in relation to the organization's exposure, the actor's capability, the credibility of the source, and the potential consequences. The analyst should determine what the information changes. It may reveal a previously unknown compromise, strengthen an existing assessment, identify a supplier supporting several threat groups, expose a new targeting preference, or show that a criminal service is losing reliability. Actionable intelligence should connect the observed activity to a practical response. That response may involve resetting credentials, investigating an endpoint, contacting a supplier, blocking infrastructure, increasing monitoring, notifying leadership, preserving evidence, or referring the matter to law enforcement.

6.1 Strategic, Operational, and Tactical Intelligence

Strategic intelligence examines broader changes in the criminal environment. It may identify the growth of a service model, the increased use of stolen sessions, the fragmentation of ransomware operations, the movement of criminal communities to private platforms, or the convergence of fraud and cyber intrusion. Strategic reporting should explain what is changing, why it matters, and how the change may affect future risk. It should avoid relying on individual advertisements as evidence of a wider trend unless several independent observations support the conclusion.

Operational intelligence focuses on specific actors, sectors, technologies, and campaigns. It may show that access brokers are increasingly offering organizations from a particular industry, that a criminal group is recruiting specialists in cloud administration, or that a malware service is expanding into a new region. Operational intelligence helps teams adjust monitoring, collection, and defensive priorities. It can also guide investigations by identifying relevant actors, suppliers, infrastructure, and likely next steps. Tactical intelligence concerns immediate indicators and specific exposure. It may include compromised accounts, active sessions, victim names, malware hashes, domains, cryptocurrency addresses, or technical details concerning access.

Tactical reporting should be timely and precise. Its value declines quickly when credentials expire, infrastructure changes, or criminal listings disappear. Where appropriate, indicators should be accompanied by context explaining how they were obtained and how reliable they are. The three levels should reinforce one another. A tactical discovery may reveal a broader operational pattern, while repeated operational observations may support a strategic assessment.

Strategic understanding can also help analysts recognize why an apparently isolated forum post is significant.

6.2 Intelligence Reporting and Escalation

Reporting should separate facts, assessments, and uncertainties. Observed information should be described clearly, while analytical judgment should be identified as such. The reader should understand what was directly observed, what was corroborated, and what remains unconfirmed. The report should explain the source and context of the information without unnecessarily exposing sensitive collection methods. It should identify the forum, actor, date, relevant content, and supporting evidence, while protecting operational details where disclosure could compromise continued access or an investigation.

Confidence language should be consistent. Analysts should avoid presenting plausible inferences as established facts. Statements such as “access was advertised,” “the credentials appeared authentic,” or “the vendor claimed a sale” are more precise than stating that the victim was definitively compromised when validation is incomplete. Escalation should reflect severity, credibility, and urgency. A vague mention of a company may require monitoring, while valid administrative credentials or evidence of active network access may justify immediate action.

A useful escalation decision should consider the asset's sensitivity, the level of access, the actor's credibility, the recency of the information, the likelihood of exploitation, and the potential impact on the victim. Reporting should also include clear recommendations. These may involve credential resets, session revocation, endpoint investigation, log review, threat hunting, supplier notification, executive protection, financial monitoring, or engagement with law enforcement.

The recommendations should be proportionate to the confidence level. Low-confidence reporting may justify enhanced monitoring, while high-confidence evidence of active access may require immediate containment and incident response. Intelligence teams should track outcomes. If a report leads to confirmation of a compromise, invalidation of a claim, or identification of a new actor, that result should be used to improve future source assessment and collection priorities.

7. Investigative Challenges and Emerging Trends

Cybercriminal forums are difficult to investigate because identities, infrastructure, and criminal relationships are deliberately obscured. Actors use pseudonyms, encrypted communications, cryptocurrency, intermediaries, and shared services to reduce the visibility of their activity. At the same time, criminal markets depend on trust, reputation, customer support, and repeated transactions. These commercial requirements create indicators that can assist in the investigation. Actors must advertise, communicate, resolve disputes, receive payments, and maintain relationships. The need to conduct business exposes even in highly anonymous environments.

7.1 Investigative Limitations

The first limitation is incomplete visibility. Analysts rarely have access to every section of a forum, every private message, or every platform an actor uses. Public content may represent only the advertising stage, while the most important negotiations occur privately. Access restrictions can create a misleading picture of a platform. A newly registered researcher may see low-level discussion while established members use private sections and invitation-only channels. The absence of visible activity does not necessarily indicate that no significant activity exists.

Attribution is also difficult because criminal identities are unstable. Accounts may be sold, shared, stolen, impersonated, or controlled by several individuals. A username can provide continuity, but it should not be treated as proof of a single real-world identity. Language presents another challenge. Criminal slang, technical terminology, transliteration, coded references, and machine translation can distort meaning. The same term may have different meanings across communities, while actors may deliberately use ambiguous language to avoid detection.

Deception is constant. Vendors exaggerate capabilities, advertise recycled data, fabricate reviews, and claim responsibility for attacks they did not conduct. Competitors may publish false accusations or impersonate trusted sellers. Analysts must assume that criminal claims may serve a commercial or reputational purpose. Technical overlap can also be misleading. Two operations may use the same malware, infrastructure, or cryptocurrency service because they purchased access from the same provider. Common tooling does not necessarily establish common control.

Financial tracing has similar limitations. Cryptocurrency transactions may pass through exchanges, mixers, brokers, cross-chain services, mule accounts, or aggregated laundering infrastructure. A wallet can represent a customer, service provider, escrow operator, or temporary collection point. Victim identification may remain uncertain where listings contain limited or deliberately obscured information. Sellers often provide only the country, sector, revenue, or technology environment. Analysts may identify several possible victims but lack sufficient information to make a confident match.

Law-enforcement disruption can create additional uncertainty. A forum may remain online under new administrators, criminal successors, scammers, or law-enforcement control. Actors themselves may not know whether a replacement platform is genuine. These limitations do not, by definition, make forum intelligence unreliable. They require analysts to combine forum observations with technical, financial, behavioral, and victim-side evidence.

7.2 Evolution of the Forum Ecosystem

The forum ecosystem is becoming more fragmented. Traditional forums remain important for discovery, reputation building, and advertising, but higher-value transactions increasingly move to encrypted messaging platforms, private groups, and invitation-only networks. This does not mean that forums are disappearing. Their role is changing. They continue to provide persistent identities, public reputation, dispute resolution, recruitment, and access to new customers. However, they increasingly function as entry points into wider criminal networks rather than as the sole location of criminal activity.

Law-enforcement actions have accelerated this fragmentation. Takedowns remove infrastructure and expose users, but the underlying relationships often survive. Vendors and customers migrate, administrators establish successor platforms, and criminal services continue under new names. The resilience of the ecosystem depends less on a specific domain than on the portability of reputation and relationships. An established actor can move to another forum while retaining the same customers, contact methods, and commercial role.

Criminal service models are also becoming more specialized. Access, malware, infrastructure, negotiation, data analysis, fraud, and money laundering can be purchased separately. This reduces the importance of large, stable criminal groups and increases the role of temporary partnerships and specialist providers. At the same time, some criminal operations are becoming more professional. They offer customer support, subscription pricing, service guarantees, affiliate panels, technical updates, and dispute mechanisms.

This professionalization does not eliminate instability. Exit scams, arrests, internal conflict, and poor security remain common. The boundaries between cybercrime, fraud, espionage, hacktivism, and state-aligned activity are also becoming less distinct. Different actors may use the same commercial infrastructure, stolen credentials, malware, and access brokers. Analysts must therefore assess intent and control rather than relying only on the tools used.

7.3 Emerging Trends

One important trend is the growing role of identity-based access. Stolen credentials, authentication cookies, session tokens, and infostealer logs allow criminals to bypass traditional perimeter controls. The value of these assets increases when they provide access to cloud environments, remote management platforms, source code repositories, or identity systems. A second trend is the continued growth of access brokerage. Initial-access brokers reduce the time other criminals need to identify and compromise victims. Their activity can provide early warning, as access may be advertised before the final attack. A third trend is the increasing separation between intrusion and monetization. The actors who comprise an organization may not be the ones who commit fraud, engage in extortion, or engage in laundering. This creates more complex investigations but also more points at which the operation may be detected or disrupted.

Fraud operations are becoming more integrated with social engineering. Stolen data is increasingly combined with impersonation, call centers, forged documents, account verification, and local financial knowledge. Artificial intelligence can improve the scale and quality of impersonation, translation, and victim interaction, but human participation remains important in complex fraud.

Criminal actors are also using automation to process stolen data. Automated checking services can test credentials, identify valuable accounts, classify victims, and prioritize access. This allows criminals to extract greater value from large volumes of low-quality data. Private criminal communities are likely to become more important. Established actors may rely less on public advertisements and more on trusted brokers, guarantors, and invitation-only groups. This may reduce public visibility while increasing the importance of long-term identity and relationship analysis. The use of legitimate commercial services will continue to complicate attribution and disruption. Cloud platforms, domain providers, communication tools, hosting services, and cryptocurrency exchanges may be used directly or through compromised accounts and resellers.

Another emerging concern is the convergence of criminal and state-aligned ecosystems. State-linked or politically motivated actors can purchase access, data, infrastructure, or malware from criminal providers. Criminal suppliers may not know the customer's identity or purpose. The resulting technical overlap can lead to false attribution if analysts assume that common tools imply a common direction. The most durable trend is the shift from identifiable criminal groups to flexible criminal networks. Brands, forums, and malware families may disappear, but experienced individuals, trusted brokers, infrastructure providers, and laundering services continue to operate. Intelligence collection should therefore focus on people, relationships, assets, and financial flows rather than relying solely on group names.

Conclusion

Cybercriminal forums are not merely online discussion spaces or digital marketplaces. They are coordination environments that transform fragmented criminal capabilities into functioning and adaptable supply chains. Through these platforms, threat actors identify partners, advertise services, establish reputations, transfer stolen assets, recruit specialists, resolve disputes, and obtain the access, malware, infrastructure, expertise, and financial services required to conduct complex operations. Their significance therefore lies less in the volume of content they contain than in the operational activity they enable. A single access listing may connect an initial compromise to ransomware deployment, fraud, espionage, extortion, or data theft. A dispute may expose an otherwise hidden transaction. A recruitment post may reveal a capability gap, an emerging operational requirement, or a future targeting priority. A cryptocurrency address, contact handle, encryption key, or reused identity may connect actors, transactions, and infrastructure across multiple platforms.

Forum intelligence must consequently extend beyond the collection of posts, aliases, and advertisements. Effective analysis requires an integrated assessment of the platform, the actor, the claim, the transaction, the supporting infrastructure, and the wider operational context. Analysts must distinguish advertising from demonstrated capability, claimed sales from confirmed transfers, and technical similarities from evidence of common ownership or control. They must also account for the increasingly decentralized and cross-platform nature of the ecosystem, in which public forums function alongside private messaging applications, invitation-only communities, automated marketplaces, data-leak sites, cryptocurrency services, and direct broker-to-buyer relationships.

Law-enforcement seizures and takedowns are an important part of this environment and should be treated as both disruption events and intelligence opportunities. The seizure of a forum, marketplace, server, or domain may interrupt transactions, undermine trust, expose communications, preserve evidence, identify users, reveal financial relationships, and support subsequent arrests or infrastructure disruption. In some cases, law-enforcement agencies may covertly control or monitor criminal platforms before publicly dismantling them, allowing investigators to map participants, transactions, access brokers, service providers, and operational dependencies. Seized databases, private messages, transaction records, cryptocurrency addresses, login information, and administrative material may provide a far more complete picture of the ecosystem than publicly visible content alone.

However, the removal of a platform does not necessarily dismantle the criminal market it served. Actors may migrate to replacement forums, private channels, or competing marketplaces; administrators may relaunch under a new name; trusted vendors may carry their reputations and customer relationships elsewhere; and buyers may reconnect with suppliers through previously established contacts. Takedowns can also produce secondary effects, including distrust, accusations of infiltration, increased vetting, stronger operational security, market fragmentation, and greater reliance on closed communities. Analysts must therefore assess not only whether a platform has disappeared, but also how its users, services, transactions, and relationships have been redistributed.

The most effective analytical approach is consequently relationship-based and ecosystem-wide. Analysts should examine how access, stolen data, malware, infrastructure, expertise, and criminal proceeds move between actors and platforms. They should identify which providers occupy central positions, which services are difficult to replace, which communities provide trust and reputation, and which operational handoffs create opportunities for early warning, attribution, intervention, or disruption. They should also evaluate the consequences of law-enforcement activity: which actors were removed, which capabilities remain available, which networks have fragmented, and where displaced activity is likely to re-emerge.

Forum monitoring has its greatest value when it supports action. This may involve protecting an exposed organization, invalidating compromised credentials, warning potential victims, identifying a criminal supplier, preserving evidence, tracing financial flows, disrupting infrastructure, supporting prosecution, or anticipating the next stage of an operation. The forum is the visible interface of the criminal market, but it is only one component of a wider system.

The more durable structure lies behind it: a network of actors, services, reputations, infrastructure, dependencies, communications channels, and financial relationships that allows cybercrime to adapt and continue even when individual platforms are infiltrated, seized, or dismantled. Understanding that broader structure is essential both for producing accurate intelligence and for designing disruption strategies that have effects beyond the temporary removal of a single forum.

About the Author



I am a Cyber Threat Intelligence expert (Crime, Warfare, Terrorism) with over 15 years of experience across academia, high-tech, military, and law enforcement environments. My core expertise includes intelligence strategy, collection, research, and analysis, with a strong specialization in leading cyber intelligence research initiatives and Cyber HUMINT operations targeting criminal and terrorist activity in cyberspace. My research interests center on cybercrime, cyberterrorism, and cyber-geopolitical intelligence. Throughout my career, I have trained numerous civilian analysts, military personnel, and law enforcement officers in cyber intelligence research and operational practices, including work in Deep and Dark Web environments, intelligence collection and analysis, and methodological frameworks.

References

1. Europol. (2026, April 28). The evolving threat landscape: How encryption, proxies and AI are expanding cybercrime—Internet Organised Crime Threat Assessment 2026. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape
2. Europol. (2025, June 11). Steal, deal and repeat: How cybercriminals trade and exploit your data—Internet Organised Crime Threat Assessment 2025. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data
3. Europol. (2024, July 22). Internet Organised Crime Threat Assessment 2024. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
4. United States Department of Justice. (2026, March 4). United States leads dismantlement of one of the world's largest hacker forums. https://www.justice.gov/opa/pr/united-states-leads-dismantlement-one-worlds-largest-hacker-forums
5. United States Department of Justice. (2025, January 30). Cracked and Nulled marketplaces disrupted in international cyber operation. https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation
6. United States Department of Justice. (2022, April 12). United States leads seizure of one of the world's largest hacker forums and arrests administrator. https://www.justice.gov/archives/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator
7. Federal Bureau of Investigation. (2016, February 10). Structure, organization, and processes of the international market for stolen data. FBI Law Enforcement Bulletin. https://leb.fbi.gov/bulletin-highlights/bulletin-reports/bulletin-reports--structure-organization-and-processes-of-the-international-market-for-stolen-data
8. Microsoft. (2025). Microsoft Digital Defense Report 2025. Microsoft. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025
9. Recorded Future. (2022, August 2). Initial access brokers are key to rise in ransomware attacks. Insikt Group. https://www.recordedfuture.com/research/initial-access-brokers-key-to-rise-in-ransomware-attacks
10. Recorded Future. (2022). 2022 annual report. Insikt Group. https://www.recordedfuture.com/research/2022-annual-report
11. Recorded Future. (2022). Session hijacking and MFA bypass: The criminal underground ecosystem for stolen cookies and credentials. Insikt Group.

https://www.recordedfuture.com/blog/session-hijacking-mfa-bypass
12. Trend Micro Research. (2025). The ever-evolving threat of the Russian-speaking cybercriminal underground. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-ever-evolving-threat-of-the-russian-speaking-cybercriminal-underground
13. Trend Micro Research. (2020). Trading in the dark: An investigation into the current condition of underground markets and cybercriminal forums. Trend Micro. https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/trading-in-the-dark
14. Sophos. (2022, December). Law, order and mayhem: Cybercriminals scam each other out of millions of dollars and take their complaints about the scams to arbitration rooms. Sophos X-Ops. https://www.sophos.com/en-us/press/press-releases/2022/12/cybercriminals-scam-each-other-out-of-millions-of-dollars
15. Flare. (2024, August). The use of large language models for cyber threat intelligence in cybercrime forums. Flare and the Université de Montréal. https://flare.io/wp-content/uploads/WhitePaper_LLM_UdeM_Flare_VF-1.pdf
16. Holt, T. J., Smirnova, O., & Hutchings, A. (2016, September 14). Examining signals of trust in criminal markets online. Journal of Cybersecurity, 2(2), 137–145. https://doi.org/10.1093/cybsec/tyw007
17. Dupont, B., Côté, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of “the most dangerous cybercrime forum in the world.” American Behavioral Scientist, 61(11), 1219–1243. https://doi.org/10.1177/0002764217734263
18. Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. International Journal of Offender Therapy and Comparative Criminology, 63(8), 1127–1147. https://doi.org/10.1177/0306624X18811101
19. Haslebacher, A., Onaolapo, J., & Stringhini, G. (2016, July 1). All your cards are belong to us: Understanding online carding forums. arXiv. https://arxiv.org/abs/1607.00117
20. Campobasso, M., Rădulescu, R., Brons, S., & Allodi, L. (2023, June 9). You can tell a cybercriminal by the company they keep: A framework to infer the relevance of underground communities to the threat landscape. arXiv. https://arxiv.org/abs/2306.05898