ZEROFOX INTELLIGENCE

Brief

Introduction to Deep and Dark Web Forums

B-2025-06-12b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Cybercrime, Deep and Dark Web

June 12, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 9:00 AM (EDT) on June 12, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | Introduction to Deep and Dark Web Forums

| Key Findings

- Deep and dark web (DDW) forums and marketplaces operate in areas of the internet that are less visible to the majority of users. While most of the domains found within these areas serve legitimate purposes, many facilitate illegal activities.
- Many DDW forums and marketplaces have undergone varying degrees of "professionalization," manifested by the widespread acknowledgement of "norms" by frequenting actors and the implementation of systems such as credibility rankings, escrow, and arbitration services.
- Instant messaging (IM) applications and platforms also fulfill a vital role in facilitating cybercrime sales and services, primarily due to the ease of accessibility, large target audiences, varying degrees of moderation, and encrypted messaging.
- DDW forums and marketplaces are almost certain to continue adapting to offer the services, accessibility, and anonymity demanded by an ever-growing number of cybercriminals, as well as minimizing the threat posed by external factors such as offensive law enforcement (LE) operations.

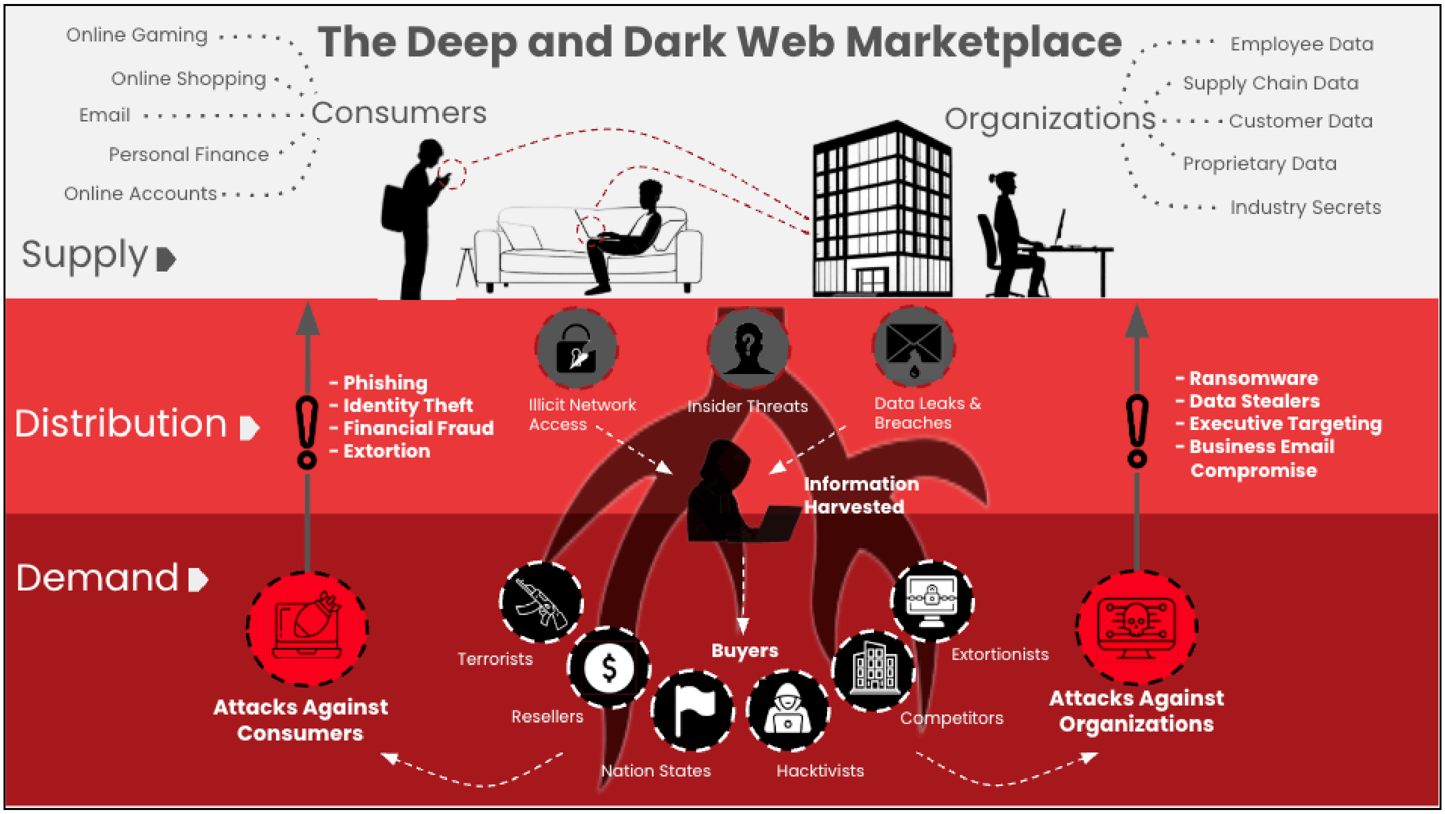
The Deep and Dark Web

The internet can be divided into three parts: the surface web, the deep web, and the dark web. The surface web can be thought of as the “visible” part of the internet that uses well-known top level domains (TLDs) such as .com and .org, as well as URLs that can be indexed via regular search engines. The deep web constitutes the vast majority of the internet and refers to web pages that cannot be indexed by regular search engines. The vast majority of these sites are perfectly legal and legitimate, consisting of private or personal pages not intended for the general public, such as email inboxes, banking data, and business intranets. Lastly, the dark web is a further-concealed subset of the deep web that is only accessible through anonymous browsers such as The Onion Router (TOR) due to its unique registry operator. Dark web sites are built atop a randomized network infrastructure and are often concealed with additional security measures, such as firewalls and encryption.

DDW forums and marketplaces are online communities that exist in these more hidden areas of the internet. Though the DDW has earned a reputation as a secretive area of the web where illegal activities proliferate, many associated forums are used to facilitate legitimate anonymous communications or bypass government censorship. However, in the context of cybersecurity and cybercrime, DDW forums are generally viewed as vibrant ecosystems where stolen data, hacking tools, and illicit services exchange hands in the shadows.

DDW forums are similar to clearnet forums in function, existing as public discussion platforms though often differing in content, with users discussing more controversial, legally nuanced, or secretive topics. Meanwhile, DDW marketplaces are where the information, drugs, and cybercrime tools are listed for sale and trade hands. Forums and marketplaces are often hosted on the same domain, and the terms are often used interchangeably.

The DDW landscape is constantly evolving, influenced by new marketplaces, high-profile actors, geopolitical factors, new technological advances, and LE activity. Despite these perpetual changes, a handful of highly frequented forums and marketplaces are responsible for trading many of the illicit services that pose a cyber threat to organizations across the globe.



Overview of the DDW marketplace
Source: *ZeroFox Intelligence*

Formalization and Professionalization

Reputation Systems

Much like “surface level” organized crime syndicates, DDW actors abide by many norms and standards which help to minimize potential losses, prevent infiltration by security services, and best benefit from each other's knowledge and expertise. This etiquette has been formalized in many forums, resulting in the use of various reputation systems and regulatory mechanisms, such as escrow services and reliability ratings.

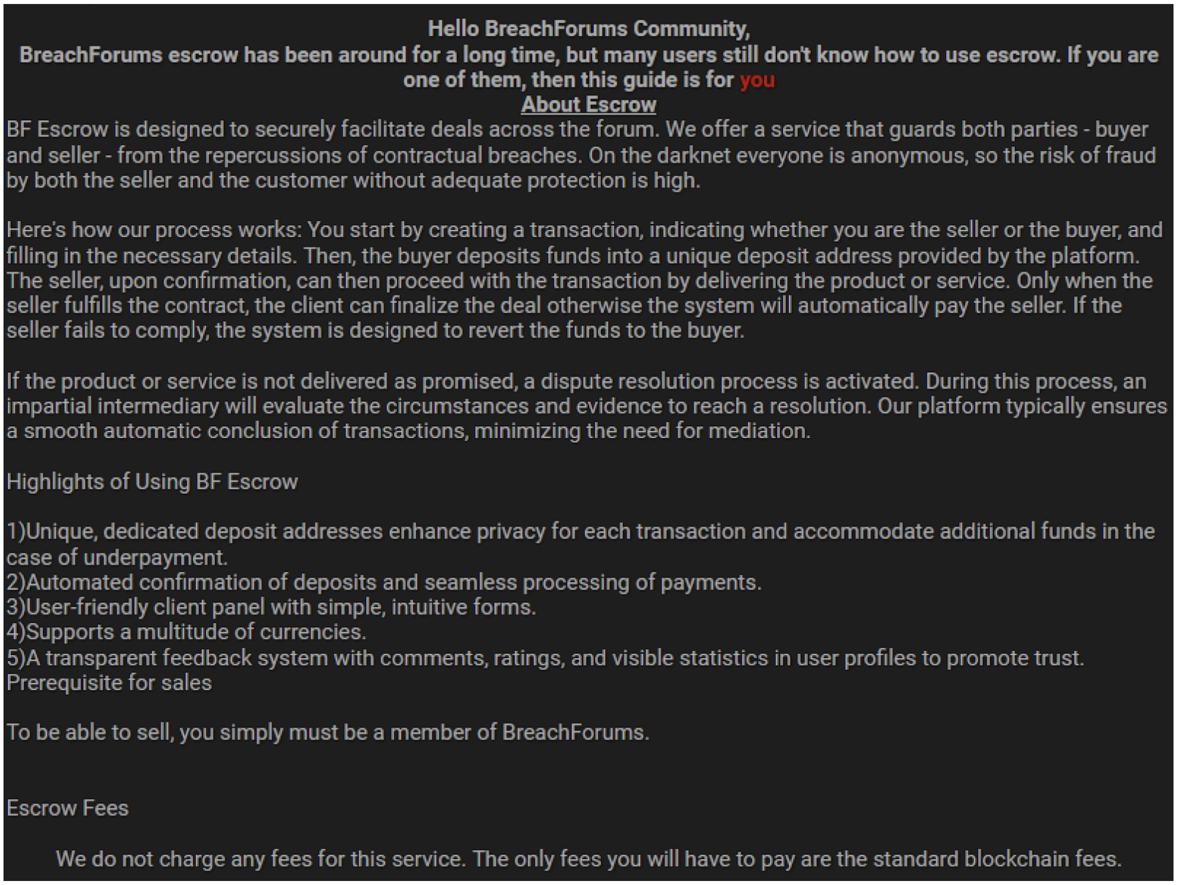
Reputation systems aim to establish trust and credibility among DDW users in an environment where traditional forms of verification are unavailable. Each forum implements these processes slightly differently, though many similarities are observed.

- The deep web hacking forum BreachForums offers users several options to bolster their reputations. The most commonly observed is the receipt of "points" from fellow users when sharing free content—an activity widespread within BreachForums. Users also gain points by participating in successful transactions or by simply purchasing a "rank," which grants a fixed reputation score.
- Peer deep web forum DarkForums operates with many similarities to BreachForums, though the purchase of a rank is not accompanied by a reputation score.
- Russian Market is an increasingly popular choice for trading stolen credentials and offers a reputation score correlated to the number of logs sold. Users' refund history is also public, adding another aspect of perceived reliability.
- Typically, obtaining reputation scores within dark web forums such as Exploit, Ramp, and xss is more difficult to achieve, as they cannot be purchased. Instead, users must partake in discussion or successful transactions or provide insight and feedback considered high-quality amongst peers. This results in reputation scores that reflect reliability more accurately than the majority of deep web forums.

Users with poor reputations often face difficulties in initiating and conducting transactions or even joining forums, since they are considered unreliable or potentially fraudulent. Users with low reputation scores or short history on the platform may be trusted with low-stakes transactions but face difficulties completing an exchange involving large sums of money. The importance of reputation systems in regulating forum behavior means DDW users must invest time in cultivating their reputations to gain the trust of other actors before they are able to conduct high-profile transactions. These relationships on the DDW often govern how information is shared. For example, a threat actor may share a breach privately with a trusted partner before sharing the information publicly on a forum.

Escrow and Arbitration Services

Another means of navigating the widespread scamming activity that takes place within DDW forums is the utilization of escrow and arbitration services, many of which are integrated and organic to the given forum. Generally, a prospective buyer and seller enter escrow after reaching an agreement on a transaction, employing a neutral third-party intermediary that receives payment from the buyer. If the buyer confirms the goods or services meet their expectations, the escrow agent releases the payment to the seller. If the content does not meet buyer expectations, the intermediary will not release the payment, and the parties will enter an arbitration process. Escrow services typically cost a small percentage of the deal total, usually between 3 to 5 percent.



Hello BreachForums Community,
BreachForums escrow has been around for a long time, but many users still don't know how to use escrow. If you are one of them, then this guide is for you
About Escrow

BF Escrow is designed to securely facilitate deals across the forum. We offer a service that guards both parties - buyer and seller - from the repercussions of contractual breaches. On the darknet everyone is anonymous, so the risk of fraud by both the seller and the customer without adequate protection is high.

Here's how our process works: You start by creating a transaction, indicating whether you are the seller or the buyer, and filling in the necessary details. Then, the buyer deposits funds into a unique deposit address provided by the platform. The seller, upon confirmation, can then proceed with the transaction by delivering the product or service. Only when the seller fulfills the contract, the client can finalize the deal otherwise the system will automatically pay the seller. If the seller fails to comply, the system is designed to revert the funds to the buyer.

If the product or service is not delivered as promised, a dispute resolution process is activated. During this process, an impartial intermediary will evaluate the circumstances and evidence to reach a resolution. Our platform typically ensures a smooth automatic conclusion of transactions, minimizing the need for mediation.

Highlights of Using BF Escrow

1)Unique, dedicated deposit addresses enhance privacy for each transaction and accommodate additional funds in the case of underpayment.
2)Automated confirmation of deposits and seamless processing of payments.
3)User-friendly client panel with simple, intuitive forms.
4)Supports a multitude of currencies.
5)A transparent feedback system with comments, ratings, and visible statistics in user profiles to promote trust.
Prerequisite for sales

To be able to sell, you simply must be a member of BreachForums.

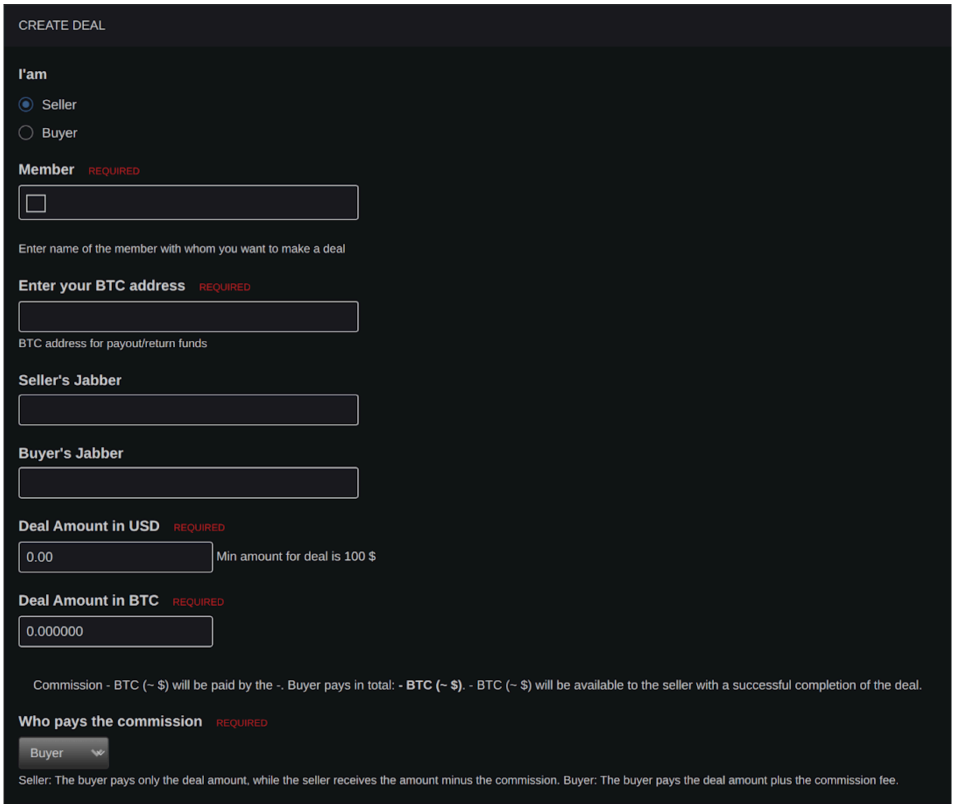
Escrow Fees

We do not charge any fees for this service. The only fees you will have to pay are the standard blockchain fees.

BreachForums escrow service

Source: ZeroFox Intelligence

Sellers often explicitly state their intent to involve escrow within any sale as a means of increasing their perceived legitimacy and standing out from those who do not. In many cases, an actor that is newly registered to a forum, or otherwise has a minimal reputation, can only attract legitimately interested buyers by offering escrow. Actors seeking to scam potential buyers by selling fabricated, misleading, or exaggerated services do not offer escrow in the majority of instances, though bans often follow such activity.



CREATE DEAL

I'am

● Seller

○ Buyer

Member REQUIRED

□

Enter name of the member with whom you want to make a deal

Enter your BTC address REQUIRED

BTC address for payout/return funds

Seller's Jabber

Buyer's Jabber

Deal Amount in USD REQUIRED

0.00 Min amount for deal is 100 $

Deal Amount in BTC REQUIRED

0.000000

Commission - BTC (~ $) will be paid by the -. Buyer pays in total: **- BTC (~ $)**. - BTC (~ $) will be available to the seller with a successful completion of the deal.

Who pays the commission REQUIRED

Buyer

Seller: The buyer pays only the deal amount, while the seller receives the amount minus the commission. Buyer: The buyer pays the deal amount plus the commission fee.

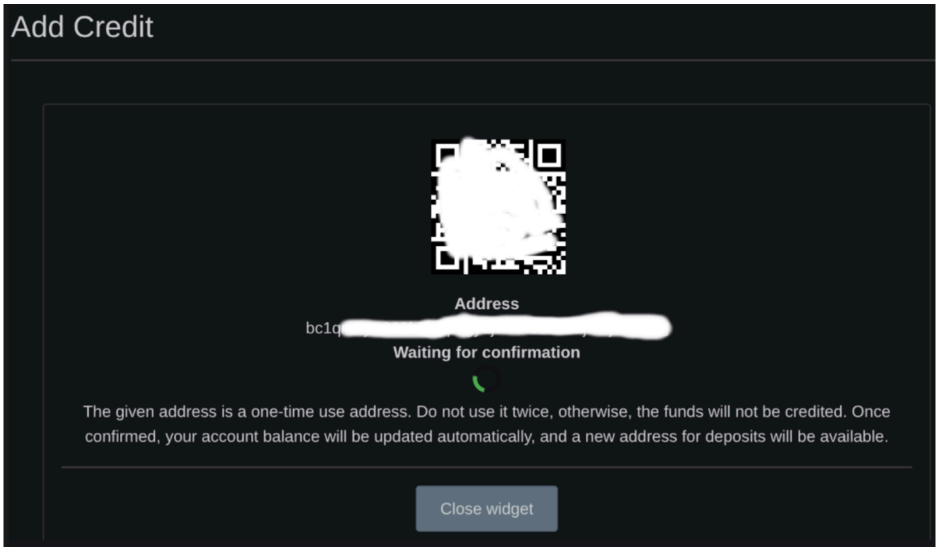
Exploit escrow service

Source: ZeroFox Intelligence

In the case of escrow services failing to deter a scam or dishonest sale, many forums utilize arbitration systems to adjudicate disputes. Arbitration acts as a pseudo court of law that presides over incidents where one party attempted to defraud another. Arbiters examine the facts of a dispute and issue a ruling on wrongdoing, if applicable. Forum administrators then enforce arbiter decisions and punish the aggressors, which can include banning them from the forum or lowering their reputations. This system helps to regulate the forum environment, where traditional arbitration channels are unavailable.

Payment Mechanisms

Transactions on DDW forums are primarily conducted using cryptocurrencies to obscure the identities of those involved. Despite operating on a public blockchain, Bitcoin (BTC) remains the favored cryptocurrency amongst DDW-dwelling cybercriminals, particularly ransomware collectives. This is most likely due to its secure hashing, as well as its widespread use and familiarity—particularly amongst potential extortion victims.



Add Credit

[redacted]

Address

bc1q[redacted]

Waiting for confirmation

The given address is a one-time use address. Do not use it twice, otherwise, the funds will not be credited. Once confirmed, your account balance will be updated automatically, and a new address for deposits will be available.

Fund deposit page on Exploit, which only accepts Bitcoin
Source: ZeroFox Intelligence

While Bitcoin is the favored cryptocurrency, others are sometimes observed being advertised as acceptable payment methods. Monero (XMR) in particular has been gaining popularity since 2022, very likely due to its enhanced anonymity and privacy features in comparison to alternatives. Litecoin (LTC) and Tether (USDT) are also used, though these are unlikely to significantly increase in popularity in the near future.

Marketplaces, Forums, and Messaging Channels

Instant Messaging Applications

Instant messaging (IM) applications and platforms play a vital role in facilitating both pre- and post-sale communications, despite being designed and used primarily for legitimate, legal activity. Some of the key reasons for their use by malicious cyber actors are as follows:

- IM platforms are often widely used and easily accessible via devices using common operating systems, such as Android and Apple's iOS. The proliferation of such applications inherently grants both buyers and sellers of malicious cyber services access to audiences that are significantly larger than those found frequenting forums—particularly those using .onion domains. Further aiding visibility, some IM platforms permit the configuration of automated marketplaces, lessening manual involvement.

- Some IM platforms, particularly in recent years, are designed and marketed under the premise of offering users a private and secure means of communicating. Many offer features such as end-to-end encryption, private/invite-only chat rooms, and the ability to register the account using no or minimal personally identifiable information (PII). While likely less secure than some dark web forums, depending on specific configurations, IM platforms can aid threat actor OPSEC and help them to avoid doxxing and LE attention.
- IM platforms have also proven to be somewhat resilient to LE intervention, reducing risk adopted by threat actors. There are a multitude of reasons for this, many of which have sparked global discussion in the spheres of right to privacy, what constitutes government overreach, the roles of IM platforms in tackling illegal activity, and the extent to which cooperation with LE entities should take place.

Telegram is one of the most popular IM platforms among cyber threat actors for some of the reasons outlined above, and it grants actors access to large channels composed of up to 200,000 people. Telegram also allows actors to register new accounts using relatively minimal user information, such as a phone number. While no true alternative to Telegram exists, actors also regularly point potential buyers of services toward other platforms such as XMPP-based Jabber or Tox, which require no personal details during registration and are based upon a peer-to-peer protocol. Sellers will often advertise initially within DDW forum and then continue communications about a prospective deal within an external messaging platform. DDW actors also frequently use forums to advertise their Telegram channels, where the actor will continuously advertise the sale of data, tools, and services.

Telegram CEO Arrest

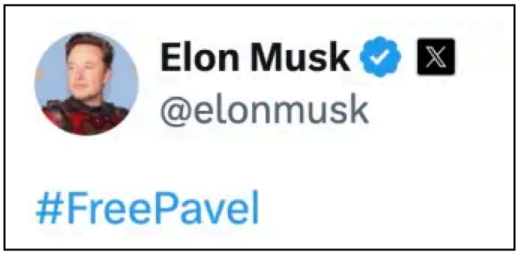
- *In August 2024, the co-founder and Chief Executive Officer (CEO) of the IM platform Telegram was arrested upon arrival in France. Days later, he was indicted on several charges, including complicity in criminal activity taking place within the platform.*
- *The arrest was largely unprecedented, and associated authorities were subject to criticism from both free-speech activists and fellow leaders of IM and social media platforms.*[1][2] *Several politicians and government officials also commented, including some from the Kremlin—who declared the arrest politically motivated due to it coinciding with the ongoing Russia-Ukraine conflict.*[3]
- *Telegram is heavily used by a wide range of cyber threat actors. Some value the privacy afforded by organic encryption and limited moderation, while others enjoy the broad exposure to wide-reaching audiences—particularly those wishing to gain notoriety or publicity (often ideologically motivated hacktivist collectives).*
- *The arrest sparked discussion surrounding legal and ethical responsibilities of both users and suppliers of IM platforms, as well as what constitutes excessive moderation.*
- *Following Pavel Durov's arrest, ZeroFox observed widespread chatter and paranoia within DDW forums, often discussing the prospect of future compromise and the ability of Telegram to continue facilitating their OPSEC requirements.*
- *No exodus of actors moving toward alternative platforms occurred, despite a marked increase in both public and private Telegram channels being banned. However, this is very likely because no like-for-like alternative currently exists.*
- *Several IM and social media platforms adjusted moderation procedures during 2024 and 2025, including making policy amendments and increasing the detection of policy violations. Adjacently, some regions implemented new legal*

[1] hXXps://x[.]com/elonmusk

[2] hXXps://www.euronews[.]com/my-europe/2024/08/26/free-speech-activists-stage-solo-protests-in-moscow-against-telegram-founders-arrest

[3] hXXps://tass[.]com/society/1834755

duties for tech companies to abide by, such as the Online Safety Act in the United Kingdom and the Digital Services Act (DSA) in the European Union (first enacted in 2022).

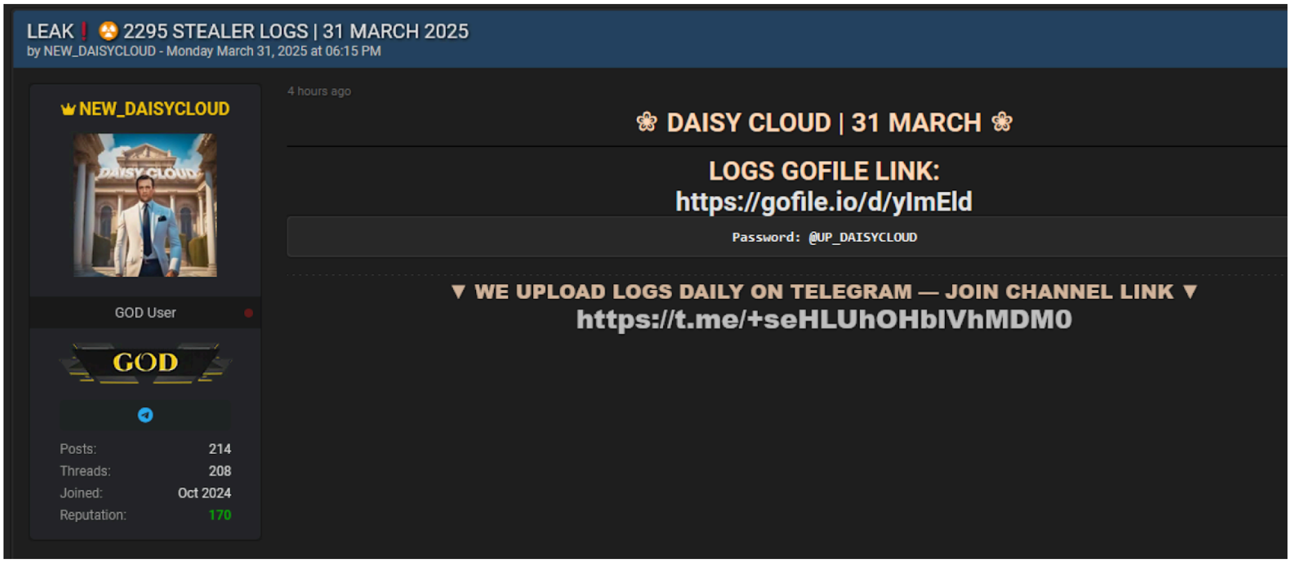


Elon Musk
@elonmusk

#FreePavel

Elon Musk supports Telegram CEO via an X post

Source: hXXps://x[.]com/elonmusk



LEAK ❗ 2295 STEALER LOGS | 31 MARCH 2025
by NEW_DAISYCLOUD - Monday March 31, 2025 at 06:15 PM

NEW_DAISYCLOUD

GOD User

GOD

Posts: 214
Threads: 208
Joined: Oct 2024
Reputation: 170

4 hours ago

❀ DAISY CLOUD | 31 MARCH ❀

LOGS GOFILE LINK:
https://gofile.io/d/ylmEld

Password: @UP_DAISYCLOUD

▼ WE UPLOAD LOGS DAILY ON TELEGRAM — JOIN CHANNEL LINK ▼
https://t.me/+seHLUhOHblVhMDM0

BreachForums user promotes their Telegram channel

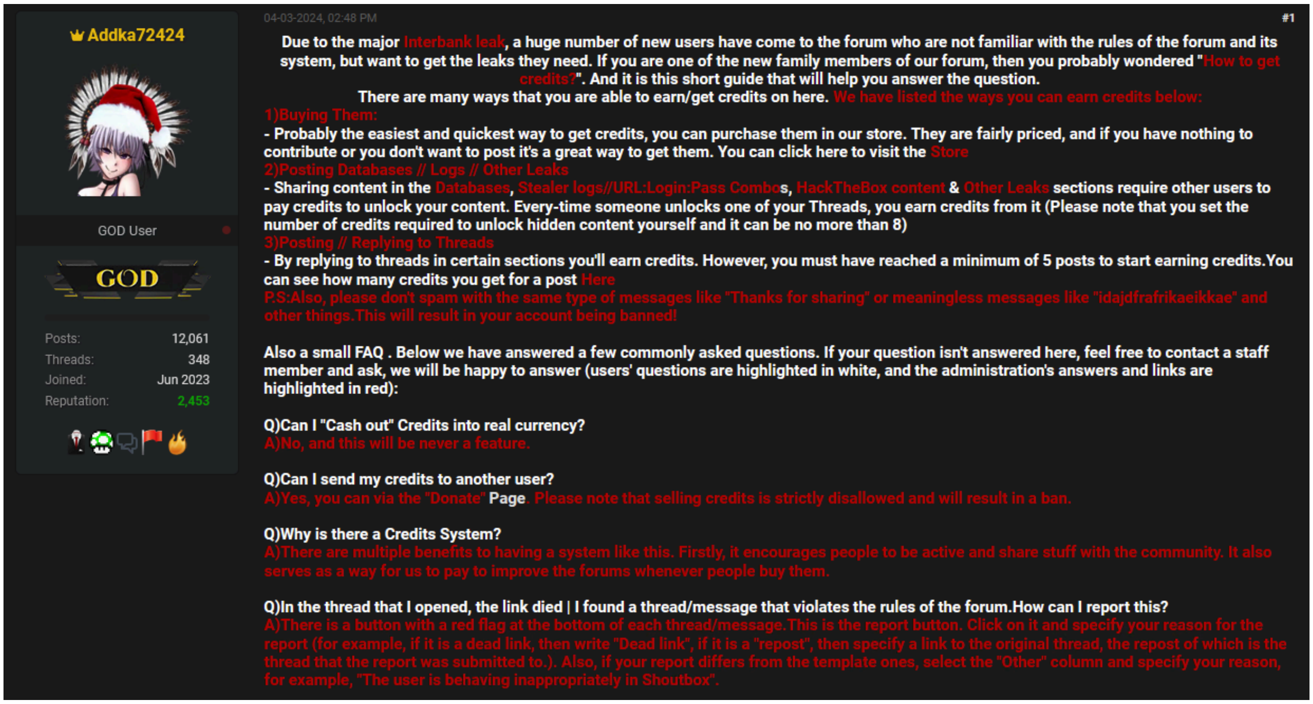
Source: ZeroFox Intelligence

BreachForums

Since its November 2022 launch, BreachForums has been one of the most popular English-language DDW forums, containing over 15 billion records from over 900 datasets and over 200,000 members. The site is frequented by both high-profile actors carrying established reputations (such as IntelBroker and Machine1337) and amateur hackers and cyber researchers. BreachForums facilitates the discussion of wide-ranging hacking topics, as well as the publication and sale of data breaches, stealer logs, hacking tools, and general discussion. BreachForums can be accessed via the surface web and TOR and does not require a verified personal account. However, the marketplace does require users to register to browse within forums or see content available for sale.

- BreachForums uses an in-forum transaction credit point system to unlock content. Users can purchase credits on the site or earn credits from posts. The forum also provides an in-house escrow system to secure transactions.
- The forum has been used to advertise numerous prominent data leaks, including those related to government, healthcare, and international non-government organizations (NGOs). Additionally, PII related to BreachForums members and administrators was leaked in July 2024.

BreachForums has experienced several severe disruptions since its launch, the majority of which have been temporary. However, around April 15, 2025, the primary BreachForums domain (.st) went offline. In the following weeks, significant discussion took place surrounding the fate of the forum, including speculation that notable members and moderators may have been arrested. A relaunch was announced on June 3, 2025, though the forum was announced for sale several days later. As of the writing of this report, BreachForums is struggling to gain traction or regain its previously established reputation.



Posts:	12,061
Threads:	348
Joined:	Jun 2023
Reputation:	2,453

04-03-2024, 02:48 PM #1

Due to the major Interbank leak, a huge number of new users have come to the forum who are not familiar with the rules of the forum and its system, but want to get the leaks they need. If you are one of the new family members of our forum, then you probably wondered "How to get credits?". And it is this short guide that will help you answer the question.

There are many ways that you are able to earn/get credits on here. We have listed the ways you can earn credits below:

1)Buying Them:

- Probably the easiest and quickest way to get credits, you can purchase them in our store. They are fairly priced, and if you have nothing to contribute or you don't want to post it's a great way to get them. You can click here to visit the Store

2)Posting Databases // Logs // Other Leaks

- Sharing content in the Databases, Stealer logs//URL:Login:Pass Combos, HackTheBox content & Other Leaks sections require other users to pay credits to unlock your content. Every-time someone unlocks one of your Threads, you earn credits from it (Please note that you set the number of credits required to unlock hidden content yourself and it can be no more than 8)

3)Posting // Replying to Threads

- By replying to threads in certain sections you'll earn credits. However, you must have reached a minimum of 5 posts to start earning credits.You can see how many credits you get for a post Here

P.S:Also, please don't spam with the same type of messages like "Thanks for sharing" or meaningless messages like "idajdfrafrikaeikkae" and other things.This will result in your account being banned!

Also a small FAQ . Below we have answered a few commonly asked questions. If your question isn't answered here, feel free to contact a staff member and ask, we will be happy to answer (users' questions are highlighted in white, and the administration's answers and links are highlighted in red):

Q)Can I "Cash out" Credits into real currency?
A)No, and this will be never a feature.

Q)Can I send my credits to another user?
A)Yes, you can via the "Donate" Page. Please note that selling credits is strictly disallowed and will result in a ban.

Q)Why is there a Credits System?
A)There are multiple benefits to having a system like this. Firstly, it encourages people to be active and share stuff with the community. It also serves as a way for us to pay to improve the forums whenever people buy them.

Q)In the thread that I opened, the link died | I found a thread/message that violates the rules of the forum.How can I report this?
A)There is a button with a red flag at the bottom of each thread/message.This is the report button. Click on it and specify your reason for the report (for example, if it is a dead link, then write "Dead link", if it is a "repost", then specify a link to the original thread, the repost of which is the thread that the report was submitted to.). Also, if your report differs from the template ones, select the "Other" column and specify your reason, for example, "The user is behaving inappropriately in Shoutbox".

BreachForums Q&A page

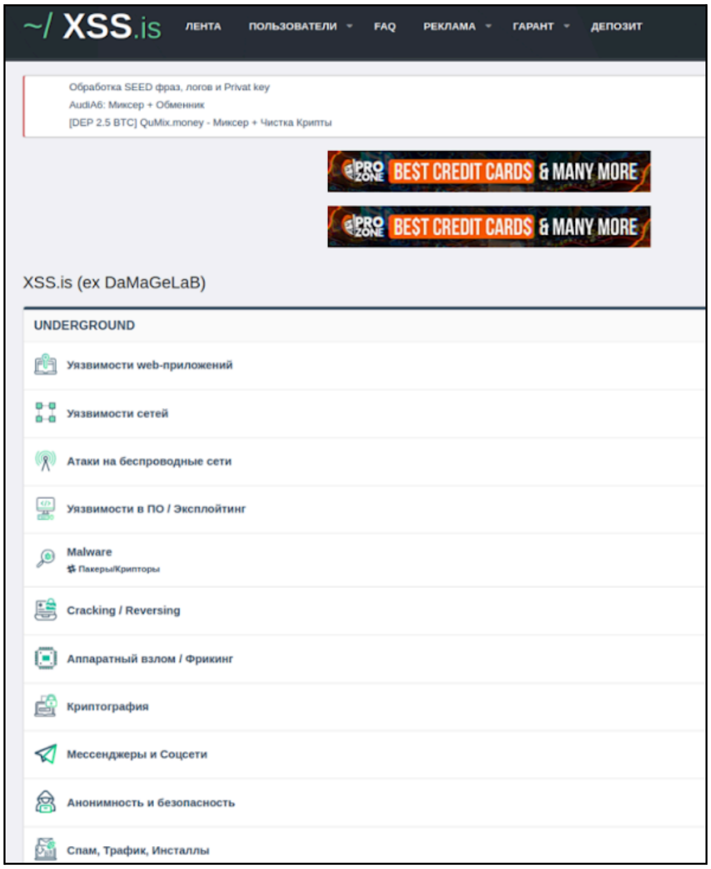
Source: ZeroFox Intelligence

Xss

Xss is a closed Russian-language forum that was founded as DaMaGeLaB in 2004, making it one of the oldest dark web forums. The site was rebranded in 2018 to xss, a name very likely associated with cross-site scripting (a web security vulnerability) and today maintains over 46,000 members. Xss is generally perceived as one of the most “professionalized” DDW forums, largely due to the rules and norms that govern the behavior of frequenting actors, as well as the nature of transactions that take place.

Generally, career criminals and state-associated actors, as well as any actor that wishes to sell or procure a valuable illicit asset such as a zero-day vulnerability, is likely to opt for a forum like xss rather than a deep web forum such as BreachForums. Xss was once a premier DDW forum for ransomware-as-a-service (RaaS) collectives to operate and hosted prominent outfits such as REvil, LockBit, and ALPHV. However, the forum banned RaaS-associated activities in 2021, which remains in place as of the writing of this report. This was very likely intended to reduce the risk of any LE scrutiny that could follow ransomware and digital extortion (R&DE) collectives—particularly those targeting sensitive targets, such as critical national infrastructure (CNI).

Today, xss enables and promotes discussions of topics such as unauthorized network access sales, malware tools, security vulnerabilities, database trading, underground job advertisements, and recruitment announcements. The forum is accessible via both surface web and .onion domains, though prospective users are required to submit a registration request that must be approved by an administrator.


~/ XSS.is
ЛЕНТА
ПОЛЬЗОВАТЕЛИ
FAQ
РЕКЛАМА
ГАРАНТ
ДЕПОЗИТ
PRO ZONE BEST CREDIT CARDS & MANY MORE
PRO ZONE BEST CREDIT CARDS & MANY MORE

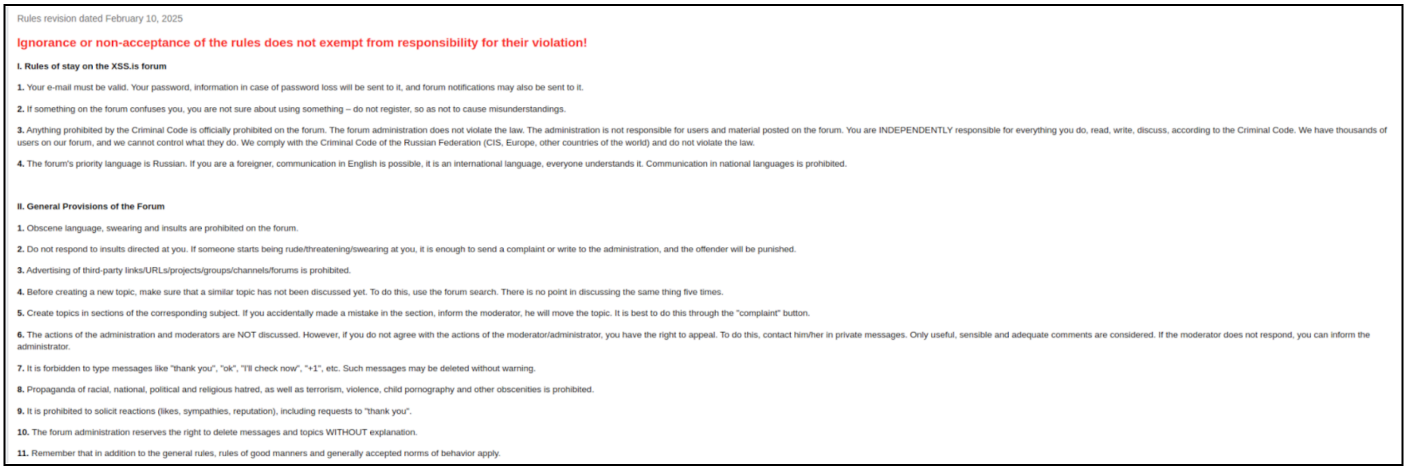
Обработка SEED фраз, логов и Privat key
AudiA6: Миксер + Обменник
[DEP 2.5 BTC] QuMix.money - Миксер + Чистка Крипты

XSS.is (ex DaMaGeLaB)

UNDERGROUND

- Уязвимости web-приложений
- Уязвимости сетей
- Атаки на беспроводные сети
- Уязвимости в ПО / Эксплойтинг
- Malware
  Пакеры/Крипторы
- Cracking / Reversing
- Аппаратный взлом / Фрикинг
- Криптография
- Мессенджеры и Соцсети
- Анонимность и безопасность
- Спам, Трафик, Инсталлы

xss homepage
Source: ZeroFox Intelligence



Rules revision dated February 10, 2025

Ignorance or non-acceptance of the rules does not exempt from responsibility for their violation!

I. Rules of stay on the XSS.is forum

1. Your e-mail must be valid. Your password, information in case of password loss will be sent to it, and forum notifications may also be sent to it.

2. If something on the forum confuses you, you are not sure about using something – do not register, so as not to cause misunderstandings.

3. Anything prohibited by the Criminal Code is officially prohibited on the forum. The forum administration does not violate the law. The administration is not responsible for users and material posted on the forum. You are INDEPENDENTLY responsible for everything you do, read, write, discuss, according to the Criminal Code. We have thousands of users on our forum, and we cannot control what they do. We comply with the Criminal Code of the Russian Federation (CIS, Europe, other countries of the world) and do not violate the law.

4. The forum's priority language is Russian. If you are a foreigner, communication in English is possible, it is an international language, everyone understands it. Communication in national languages is prohibited.

II. General Provisions of the Forum

1. Obscene language, swearing and insults are prohibited on the forum.

2. Do not respond to insults directed at you. If someone starts being rude/threatening/swearing at you, it is enough to send a complaint or write to the administration, and the offender will be punished.

3. Advertising of third-party links/URLs/projects/groups/channels/forums is prohibited.

4. Before creating a new topic, make sure that a similar topic has not been discussed yet. To do this, use the forum search. There is no point in discussing the same thing five times.

5. Create topics in sections of the corresponding subject. If you accidentally made a mistake in the section, inform the moderator, he will move the topic. It is best to do this through the "complaint" button.

6. The actions of the administration and moderators are NOT discussed. However, if you do not agree with the actions of the moderator/administrator, you have the right to appeal. To do this, contact him/her in private messages. Only useful, sensible and adequate comments are considered. If the moderator does not respond, you can inform the administrator.

7. It is forbidden to type messages like "thank you", "ok", "I'll check now", "+1", etc. Such messages may be deleted without warning.

8. Propaganda of racial, national, political and religious hatred, as well as terrorism, violence, child pornography and other obscenities is prohibited.

9. It is prohibited to solicit reactions (likes, sympathies, reputation), including requests to "thank you".

10. The forum administration reserves the right to delete messages and topics WITHOUT explanation.

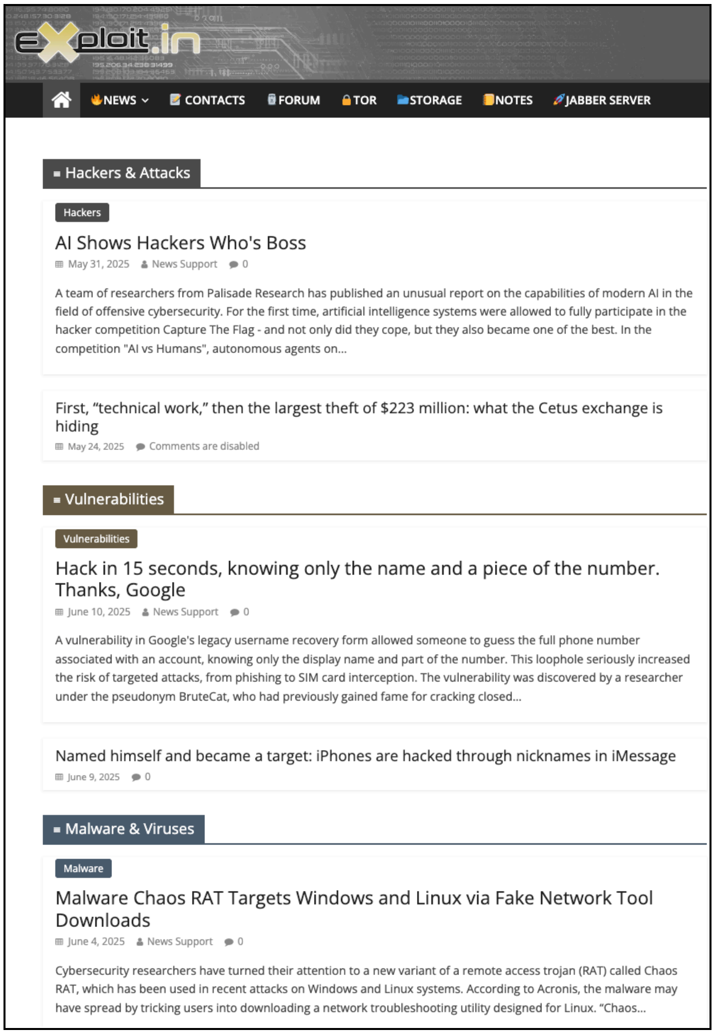
11. Remember that in addition to the general rules, rules of good manners and generally accepted norms of behavior apply.

xss membership rules

Source: ZeroFox Intelligence

Exploit

Exploit is another closed Russian-language forum dating back to 2005 that shares many similarities with xss. Exploit offers much of the same types of goods and services as xss (stolen data, malware tools, and initial access points) and is also more tailored to career-oriented cybercriminals than other forums. Moreover, Exploit also prohibits RaaS activities. To gain access to the forum, prospective members must submit an application and pay a fee (around USD 100), or they can avoid the fee by demonstrating a good reputation on different platforms. Exploit currently maintains over 66,000 registered members.



Hackers & Attacks

Hackers

AI Shows Hackers Who's Boss

May 31, 2025 News Support 0

A team of researchers from Palisade Research has published an unusual report on the capabilities of modern AI in the field of offensive cybersecurity. For the first time, artificial intelligence systems were allowed to fully participate in the hacker competition Capture The Flag - and not only did they cope, but they also became one of the best. In the competition "AI vs Humans", autonomous agents on...

First, "technical work," then the largest theft of $223 million: what the Cetus exchange is hiding

May 24, 2025 Comments are disabled

Vulnerabilities

Vulnerabilities

Hack in 15 seconds, knowing only the name and a piece of the number. Thanks, Google

June 10, 2025 News Support 0

A vulnerability in Google's legacy username recovery form allowed someone to guess the full phone number associated with an account, knowing only the display name and part of the number. This loophole seriously increased the risk of targeted attacks, from phishing to SIM card interception. The vulnerability was discovered by a researcher under the pseudonym BruteCat, who had previously gained fame for cracking closed...

Named himself and became a target: iPhones are hacked through nicknames in iMessage

June 9, 2025 0

Malware & Viruses

Malware

Malware Chaos RAT Targets Windows and Linux via Fake Network Tool Downloads

June 4, 2025 News Support 0

Cybersecurity researchers have turned their attention to a new variant of a remote access trojan (RAT) called Chaos RAT, which has been used in recent attacks on Windows and Linux systems. According to Acronis, the malware may have spread by tricking users into downloading a network troubleshooting utility designed for Linux. "Chaos...

Exploit homepage

Source: ZeroFox Intelligence

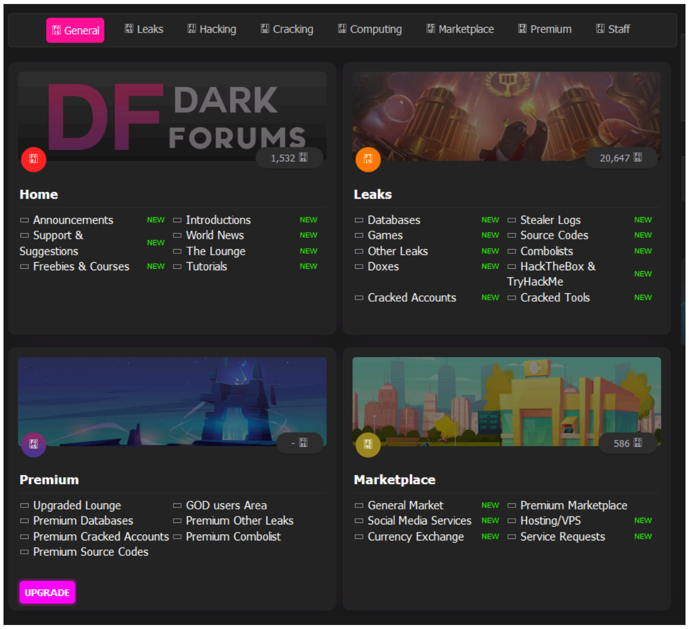
Russian Anonymous Market Place

Russian Anonymous Market Place (RAMP) was created in 2021 and, as the name suggests, is a primarily Russian-language forum. However, in recent years, English and Mandarin have also become prominent on the forum. RAMP offers much of the same goods, services, and discussions that can be found in xss and Exploit but notably allows RaaS activity. As a result, many ransomware syndicates maintain a presence on RAMP.

RAMP employs stringent membership policies to maintain the privacy of the forum; all prospective members must provide their xss and Exploit personas, as well as answer several questions—including technical questions intended to prove a candidate's expertise. In some cases, interested users may pay a USD 500 registration fee to bypass some requirements.

DarkForums

DarkForums is a deep web forum launched in 2023, which shares many similarities with BreachForums. Discussions taking place within the forum revolve around topics such as stealer logs and source codes, and multiple advertisements of stolen data sets for sale are observed on the forum. DarkForums has struggled to gain traction in comparison to other forums, though many users have been observed migrating to DarkForums in response to the disruption of BreachForums in recent weeks. This trend will almost certainly continue, even if BreachForums is able to re-establish functionality.



Home

- Announcements NEW
- Support & Suggestions NEW
- Freebies & Courses NEW
- Introductions NEW
- World News NEW
- The Lounge NEW
- Tutorials NEW

Leaks

- Databases NEW
- Games NEW
- Other Leaks NEW
- Doxes NEW
- Cracked Accounts NEW
- Stealer Logs NEW
- Source Codes NEW
- Combolists NEW
- HackTheBox & TryHackMe NEW
- Cracked Tools NEW

Premium

- Upgraded Lounge
- Premium Databases
- Premium Cracked Accounts
- Premium Source Codes
- GOD users Area
- Premium Other Leaks
- Premium Combolist

Marketplace

- General Market NEW
- Social Media Services NEW
- Currency Exchange NEW
- Premium Marketplace
- Hosting/VPS NEW
- Service Requests NEW

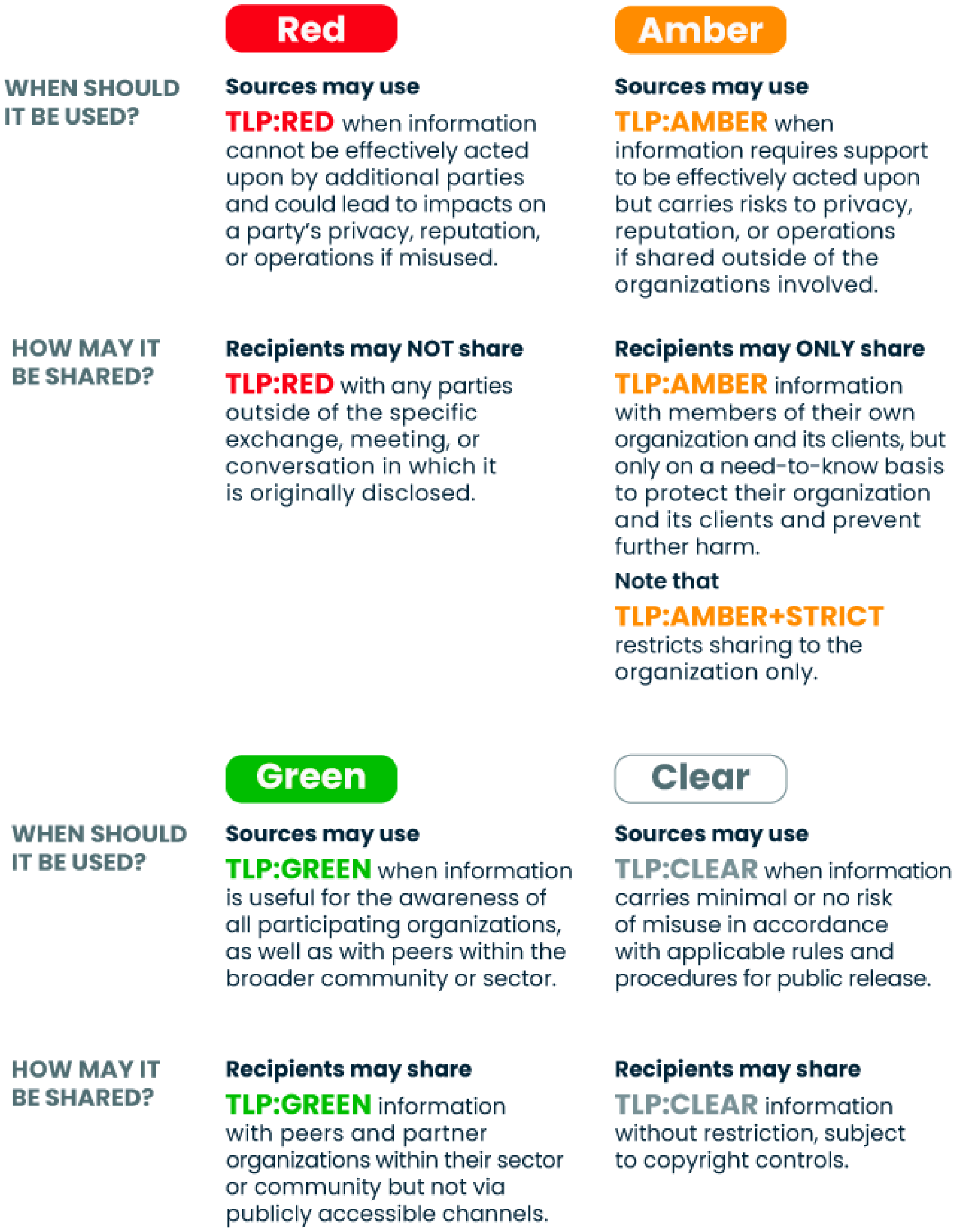
DarkForums homepage

Source: ZeroFox Intelligence

Outlook

The overall quantity of actors leveraging DDW forums and marketplaces is almost certain to increase as cybercrime proliferates and global attack surfaces grow. The DDW ecosystem will always adapt to serve user demands and withstand disruption, whether from LE entities or opposing cybercriminals. As with any commercial industry, DDW forums and marketplaces will innovate new features, such as more secure privacy mechanisms and data types, in response to consumer preferences. The same logic can be applied to forum disruptions; when one forum disappears or faces severe disruption, users will migrate to other existing platforms or create new ones. DDW forums will also always cater to varying levels of "professionalism." Forums such as xss, RAMP, and Exploit will cater to more professional and advanced cyber threat actors, while forums such as BreachForums and DarkForums will cater to more "amateur" or unproven actors-though exceptions will always exist. Users across all these platforms can be expected to employ IM platforms to drive sales and communicate with broader audiences, as long as the platform is perceived to sufficiently satisfy their OPSEC requirements.

Appendix A: Traffic Light Protocol for Information Dissemination

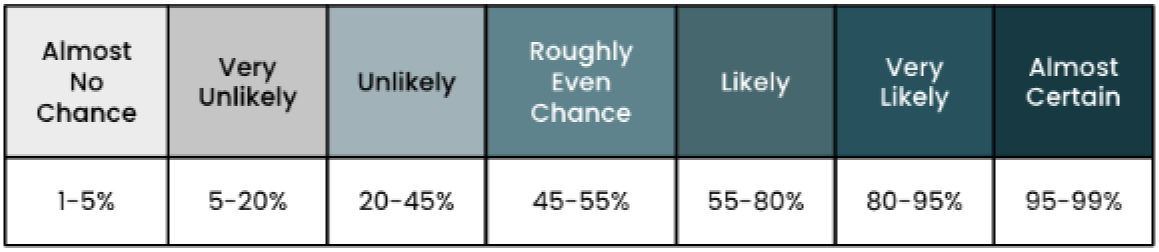


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%