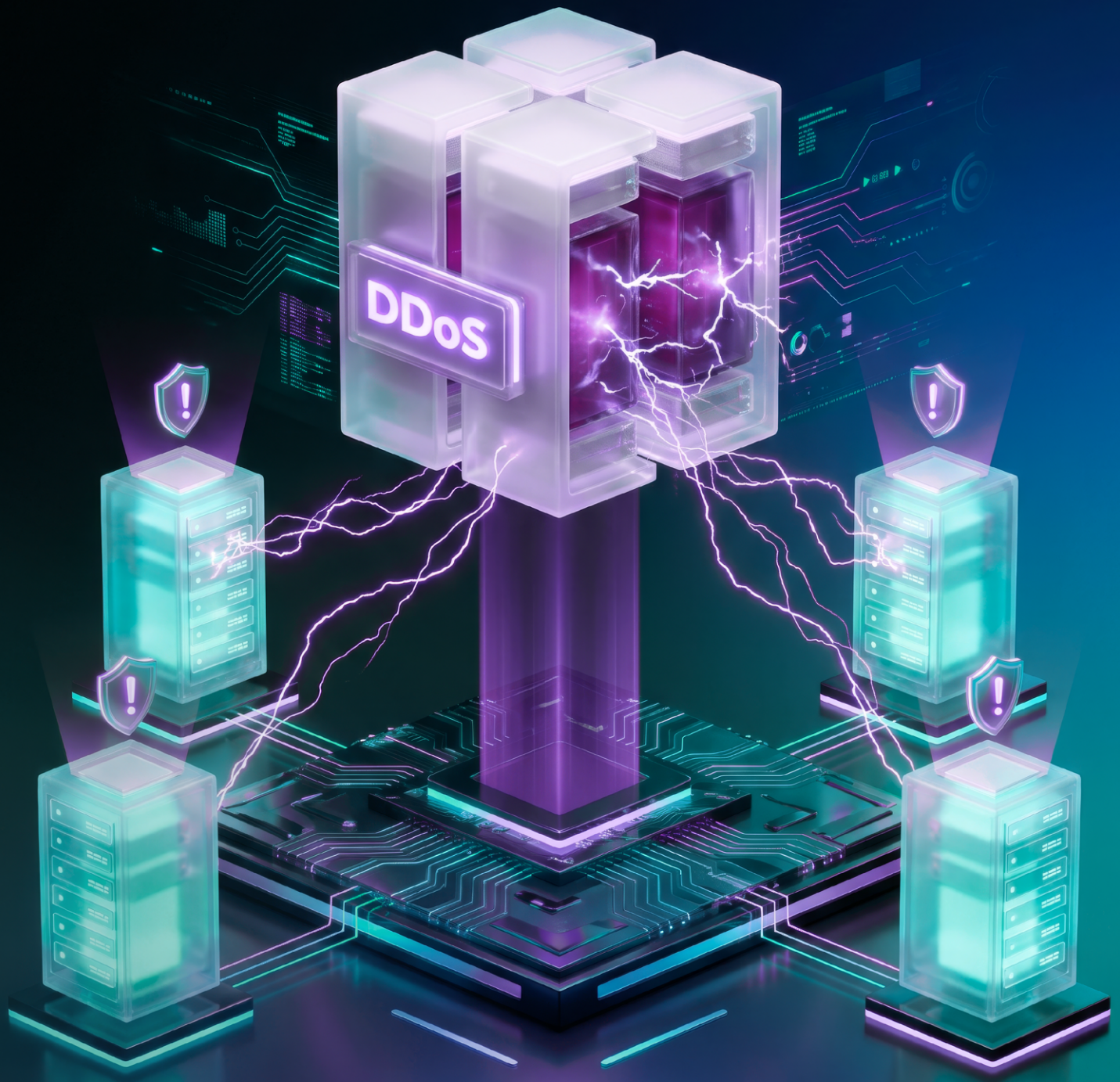




OverDDoSe

The market of flooding for profit

Introduction

The rise of DDoS attacks¹ has become a significant concern for the cybersecurity industry. Yet the attacks themselves reveal only part of the picture. Behind them lies an underground market that packages disruptive capability as a service, making targeted attacks available for a price lower than your favorite streaming service.

To examine this market, we analyzed more than 256,000 posts across the dark and deep web and identified 148 DDoS actors active since at least 2024. But the deeper story only emerged when we traced them back to 2015. Across years of advertisements, their playbooks, offers and recurring identities, a pattern took shape: this was not simply a collection of attack services, but an underground economy of disruption — persistent, adaptive and far more organized than it first appeared. In the following pages, we map its techniques, its victims, its merchants, its prices and the evolution that kept it alive.

The report unfolds in three main parts:

Means of disruption opens with the attacks themselves: the forms they take, the targets they pursue and how actors acquire the launching capability.

The destructive power price turns to the commercial side of disruption, tracing how different service models are priced and sold and how competition shapes them over time.

Survival in the trade looks at the actors behind these operations: how long they remain active, how they compete for visibility, how they stretch DDoS capability into adjacent services and how they adapt their offers as time flows.

This material was developed for technical and strategic cybersecurity experts, from threat intelligence analysts to information security managers.

¹<https://blog.cloudflare.com/ddos-threat-report-2025-q4/>

Means of disruption

Instruments of overload

Looking at how actors describe their services, we identified two broad attack categories: **L3/L4** and **L7**. Alongside them, we identified two narrower ones: **game server** attacks and **onion** attacks, which appear as specialized cases of these broader groups. Of 148 actors in our dataset, 91 specified enough detail in their advertisements for us to determine the category. In 20 of these 91 cases, the attack type was not stated explicitly but could be implied from the anti-DDoS solutions mentioned or other contextual clues.

L3/L4

L3/L4 attacks aim to overwhelm network capacity by generating high-volume traffic.

In our dataset, **L3 attacks** were relatively rare as a standalone category. In most cases, actors group L3 and L4 together, so we mainly treated them as a single category. Only **9% of actors** explicitly offered L3 methods such as ICMP, GRE, or ESP floods. **L4 attacks** were much more common: **74%** of actors mentioned TCP ACK/SYN, UDP floods, DNS amplification or other transport-layer methods.

10 Gbps–8.2 Tbps

- attempts to overwhelm network bandwidth
- simpler to execute
- easier to detect
- causes huge spikes in traffic

Games*

special case of L3/L4

1+ Tbps

*specifically crafted UDP packets

A notable case here is the **game server** attack. Technically, it fits within L4,² but actors often treat it as something separate. That is partly because game servers behave differently from ordinary web infrastructure. They consume more memory, cause spikes in CPU usage and hit disks heavily. Furthermore, game attacks often require game-specific packets, usually over UDP. This is why actors often present game attacks not as just another flood method, but as a distinct capability.

²While DDoS attacks against game servers may involve both L4 and L7 techniques, only L4 game attacks were explicitly mentioned in the advertisements.

L7

L7 attacks work differently. Instead of trying to overwhelm bandwidth or connection handling, they put pressure on the application itself.

L7 was the most commonly advertised category in our dataset: **92%** of actors claimed to offer it. One reason is that there are plenty of ready-made open-source L7 methods, which lowers the barrier to adjust it and offer it for sale. Another reason is the relative simplicity of target initialization, as launching such an attack requires little more than a target website.

Attacks on **.onion** resources are a specific case of L7 attacks, as attackers exploit the way Tor handles connections rather than relying on traffic volume alone. Just **3%** of actors could claim to implement this feature.

100,000 rps–
8,500,000 rps

- attempts to exhaust application resources
- mimics legitimate behavior
- harder to detect
- requires target understanding

.onion*

special case of L7

*requires TOR communication

Hunters and hunted

Similar DDoS methods may be driven by different motives, depending on who initiates the attack, what they are trying to achieve, and who stands in their way. Although they follow different logic, attack initiators converge on the same outcome — deliberate disruption. The main attacker profiles identified in our dataset are outlined below.

Economically hostile actors:

Cause financial loss by disrupting service availability and damaging reputation.

Harm search rankings and deplete advertising budgets via illegitimate traffic.



Ransom operators:

Force payment by disrupting services or threatening continued disruption.

Gain financially by pressuring victims to pay to stop or avoid the attack.



Hacktivists:

Draw attention to an event or “punish” organizations based on ideology.

Promote political or social views by interrupting operations and gaining public visibility.



Opportunists:

Use disruption as a distraction to enable other malicious activities or gain in-game advantage.

Situational or personal gain.



Buying the arsenal

Looking at how actors launch attacks, three models appear: brokered DDoS, DDoS-as-a-Service and in-house infrastructure. The first two depend on third-party **resource providers**, while the third belongs to actors who can build and maintain an attack infrastructure on their own.

Resource provider – an actor who already controls the infrastructure required for attack.

Brokered DDoS



attack conducted by another actor after direct communication

DDoS-as-a-Service



access to resources by subscription

In-house infrastructure



resources are self-maintained

Brokered DDoS

The most direct model is also the simplest one: an **attack initiator** contacts a resource provider and asks for an attack to be carried out. This way, DDoS brokers serve as resource providers. The first contact may happen on a dark web forum, but communication then moves to another platform – mostly Telegram or Discord. In this model, the provider handles everything from the technical side: what method to use, how to shape the traffic, and how to deal with anti-DDoS protection.

Attack initiator – an actor who intends to target a system, service or online resource with an attack.

Brokered DDoS



65%



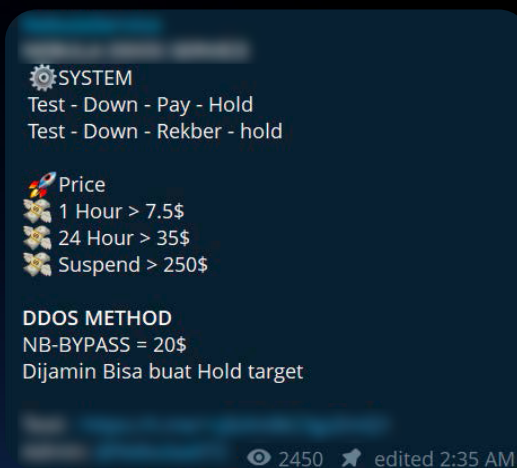
29%



6%

* based on 57 actors

Among the **57 actors** in our dataset who offered to carry out a DDoS, **65%** still relied on cybercriminal forums as their main advertising platform. The rest used messengers, mostly **Telegram** and **Discord**.



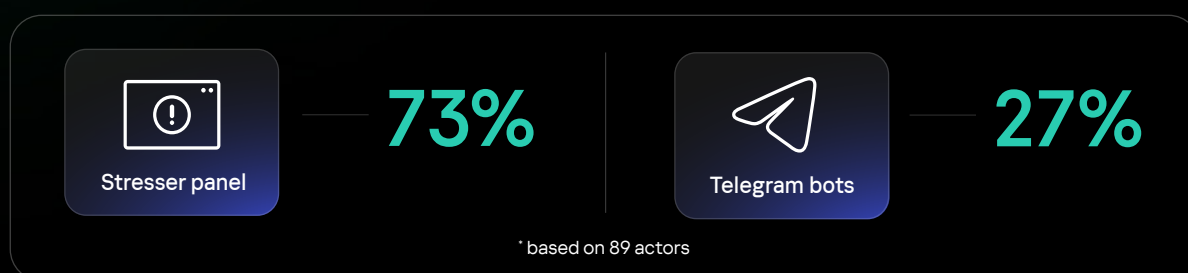
Example of brokered DDoS promotion

DDoS-as-a-Service

The second approach removes direct interactions. Instead of negotiating with a provider, the attack initiator buys access to a **stresser panel** or a **Telegram bot** and launches an attack of their own. This way, they decide on the **subscription plan**, which includes particular attack methods, the duration, and the number of concurrent attacks. Some services go further with simplifying attack initiation. For example, a basic test attack can be launched for free with a single command in a chat.

Stresser panel — an interface used to run and manage attacks in DDoSaaS, controlled by a resource provider.

Historically, this model was about web-based **stresser panels**. Since 2022, we have observed a sharp rise (in comparison with previous years) of actors advertising **Telegram bots** with dedicated DDoS functionality. Part of the market is clearly moving from websites toward simpler, faster and rapidly-renewable interfaces.



ATTACK PANEL

TARGET

ATTACK METHOD

PORT

Required - Enter port number

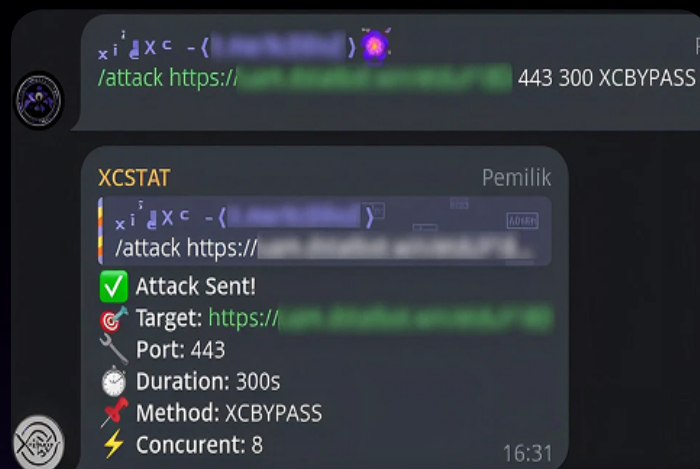
DURATION

60 seconds

CONCURRENTS

1 concurrent

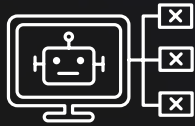
Example of a stresser panel interface



Example of attack initiation via Telegram bot

In-house infrastructure

Not all attack initiators rely on outside providers. Instead, they use their own infrastructure. In practice, this usually means that they either run attack scripts implementing one or several methods or build and maintain the entire botnet.



Botnet-based

The difference is partly technical, partly operational. A script may be enough for a narrow task or a short campaign. A botnet is different: it has to be built, maintained, and kept alive. That is why botnet-based capabilities are typically associated with more technically capable actors.



Script-based

As of April 2026, we identified over 1,000 Github repositories containing stresser scripts, along with 500 more that claimed to contain botnet source code. Scripts are widely available for free, which lowers the barrier for actors who already have technical skills. Botnets, in contrast, are rarely distributed openly and are more often sold.

The destructive power price

Different ways of acquiring DDoS capability come with different payment models. In brokered DDoS, payments are arranged per request. In DDoSaaS, the prices are standardized by fixed subscription plans.

Brokered DDoS

In **brokered DDoS**, precise **prices** are discussed **case by case**. The attack initiator contacts the provider, who examines the target before deciding on the attack cost.

Among **36 actors** in our dataset who used this model, attack prices ranged from **\$30 to \$2,000** depending on the duration, the target and the claimed strength of the service.

\$30–\$2,000

on-demand payment
for a single attack

* price range for attacks of 1 - 30 days duration

\$10

test attack

\$100

for 1 day

\$500

for 7 days

\$1250

for 30 days

* average prices based on 36 actors with on-demand payment type

A typical offer includes a short-term test attack. Some actors advertise free testing, while others charge about \$10 to let the attack initiator verify that the service works as advertised before paying for a larger campaign.



27-09-25, 06:09 PM

[Image: AuTRCMY.png]

We can do DDoS attacks on **any targets**: WEB (cleartnet), VPS/VDS, IP-TV, TCP/UDP Applications.

Why you should to choose our service?

- Always online;
- Money back is possible (if something went wrong on our side);
- Free test attack (5-10 minutes);
- We agree on the escrow;
- Round-the-clock monitoring of the attacked target.

Show Content

Prices:
Easy targets — \$50/24 hours, \$250/7 days, \$1000/30 days;
Middle targets — \$75/24 hours, \$500/7 days, \$2000/30 days;
Hard targets — individually.

Posts: 28
Threads: 1
Joined: Sep 2025
Reputation: 0
6 Months

MEMBER

Example of brokered DDoS advertisement

DDoS-as-a-service

The **subscription model** offers a wider spectrum of plans than brokered DDoS. In this case, the attack initiator pays for **access to attack capability** rather than for a single requested attack. A subscription, typically for 30 days, defines the available methods, the maximum duration of a single attack, the number of concurrent attacks, and API access. Higher tiers price plans extend limits in these parameters rather than changing the model itself.

\$1–\$30,000

subscription to attack capability
limited by plan

* for plans of 30 days duration

In our dataset, **64 actors** advertised DDoSaaS pricing. For a 30-day subscription, prices ranged from **\$1 to \$30,000**. A few actors also offered a 7-day subscription, although this was much less common. The stated duration of a single attack ranged from **1 minute to 48 hours**.

\$20

for 60s - 600s

\$191

for 300s-3,600s

\$2,160

for 3,600+ s

* average prices for one month subscription based on 64 actors

One detail appeared in these services again and again — attack duration was listed in seconds, not minutes or hours, which seemed a bit unusual. According to our observations, it comes from older DoS scripts, shaped by Unix/POSIX-style tooling, where seconds were the default time unit and plain integer seconds were simply the easiest format to work with.

IP Stresser Pricing – Best Stresser Plans

affordable stresser plans · cheap ip stresser · best stresser value

Rapid

-20%

\$8 / 31 days ~~\$10~~

IP stresser with up to 5M RPS stress power

concurrents

1

max test time

300s

api access

enabled

Choose Rapid

Felicity

-20%

\$144 / 31 days ~~\$180~~

Best stresser plan – up to 30M RPS power

concurrents

15

max test time

10400s

api access

enabled

Choose Felicity

Testarossa

-20%

\$800 / 31 days ~~\$1000~~

Powerful stresser – up to 100M RPS stress testing

concurrents

100

max test time

14400s

api access

enabled

Choose Testarossa

Best IP stresser for authorized stress testing only. Use this stresser service responsibly on your own systems.

Example of stresser panel subscription prices

Service model	What is paid for	Buyer efforts	Single attack duration	Relative cost
Brokered DDoS	A requested attack against a single target	Relatively low as the provider handles the attack	1, 7, 30 days, or entirely custom	More cost-effective for longer attacks and complicated targets
DDoSaaS	30-day access to attack capability under plan limits	Buyer chooses the method and the required power, and may need to relaunch attacks	1 min - 24h, depending on the chosen plan	More cost-effective for shorter attacks and simpler targets

Caliber of the attacks

Claims about attack capacity were found almost exclusively in DDoSaaS advertisements. DDoS brokers rarely expose this detail and attackers with in-house capability decide for themselves, which means the analysis below is primarily based on services conducted via [stresser panels](#).

In this part of the market, power is often sold through numbers: providers promise attack capacity within 15 Gbps – 7,000 Gbps range, while listed prices ranged from \$30 to \$4,500.



Among [stresser panels](#) that mentioned capacity, [36%](#) claimed [Tbps-scale](#) attacks. However, these numbers should be interpreted carefully. Capacity is something that is easy to advertise but much harder to verify. Commercial panels prefer to target mid-tier L3/L4 attacks for quick profit. Record-breaking Tbps-scale attacks are launched by state actors aiming for disruption, not pay-per-use models.

Coin of the trade

Explicit payment information was found mainly in DDoS-as-a-Service advertisements, where actors had to automate access to their services. Brokered offers were far less likely to disclose such details publicly.

The services from our dataset accepted 25 different payment methods. Most of them were cryptocurrencies. **Bitcoin** was accepted by **92%** of providers, while **60%** accepted **Ethereum** and **Litecoin**. Payment methods other than cryptocurrencies appeared much less often — just **7%**, as they do not provide enough privacy.

Most accepted cryptocurrencies



92%

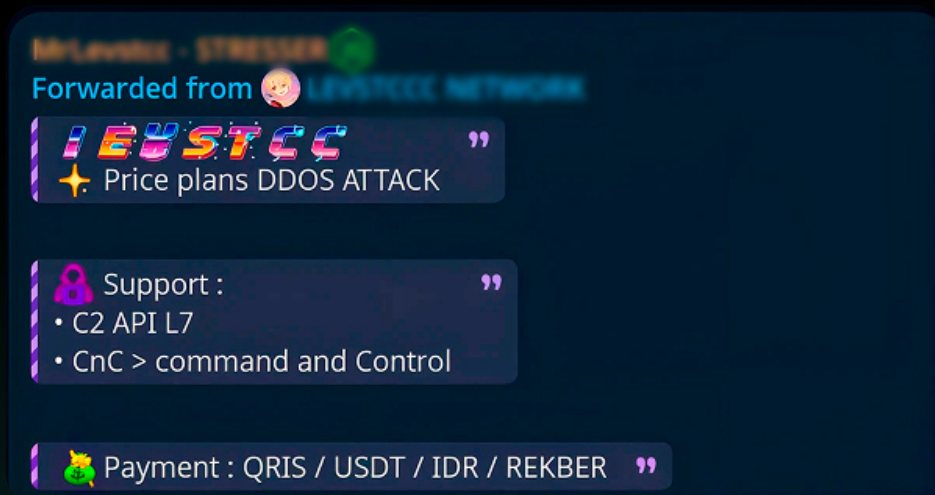


60%



60%

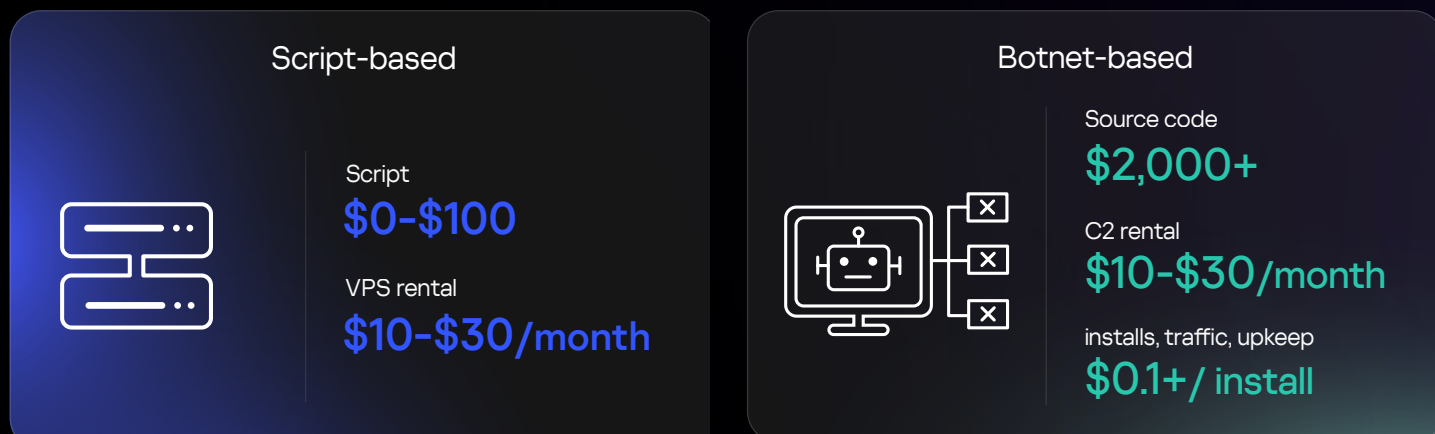
At the same time, uncommon payment methods are useful for attribution.



Example of message with specified payment methods

In-house infrastructure

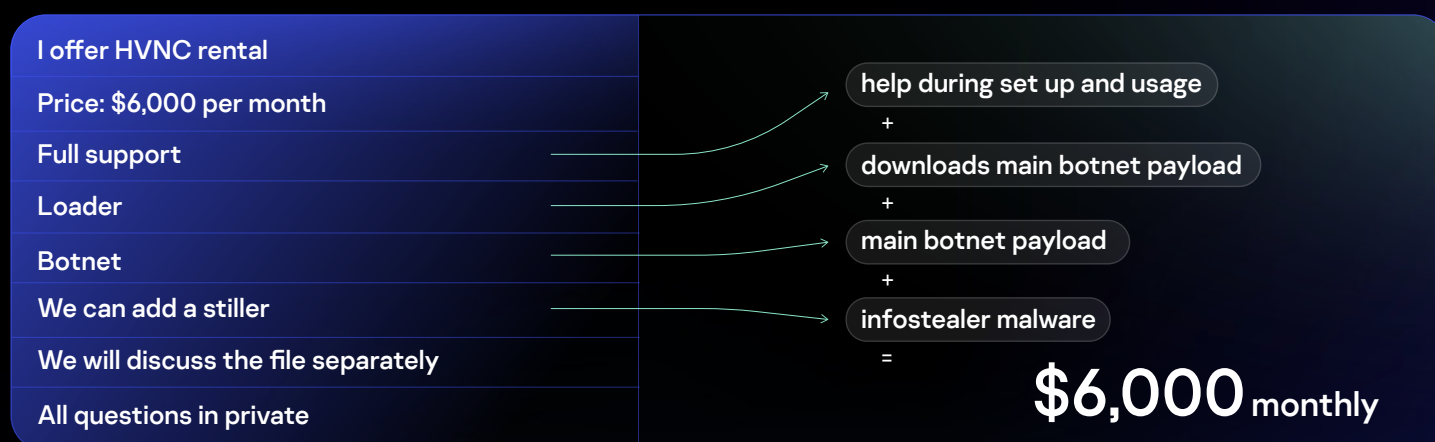
Attack initiators who rely on their **own infrastructure** face costs of a different kind. There is no single paywall, no convenient subscription or unified purchase flow. Instead, they combine attack capability out of different parts: scripts, servers, control infrastructure, and infected devices for the case of botnets. Based on the attacker's playbooks, there are two broad models to build an infrastructure: a simpler script-based setup and a more expensive botnet-based one.



In the simpler case, an actor deploys an **open-source** or **low-cost** attack **script** on rented server(s). The real expense comes from the infrastructure behind it. Hosting costs depend on the number of servers used, their characteristics, and the hosting provider's tolerance for abuse reports.

A **botnet** setup requires investment in a different league. An archaic source code can be discovered online, but a more capable botnet is usually paid rather than distributed for free, with prices starting at around \$2,000.

And that is only the tip of the iceberg. Running a botnet also means paying for C2 servers, installs, traffic, regular obfuscation to bypass antiviruses and ongoing maintenance. Unlike a script-based setup, a botnet is not just launched — it has to remain alive.



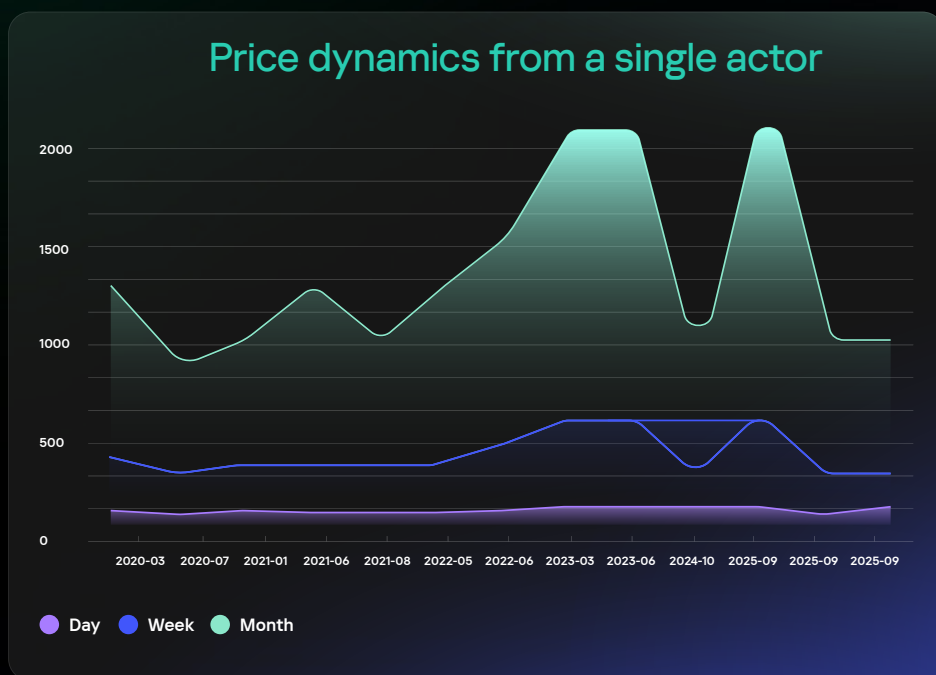
Advertisement of a botnet rental from a dark web forum

An example of a botnet advertisement shows what the rental price may include. In this case, a botnet rental package priced at \$6,000 per month included not only access to the botnet itself but also a loader, operator support and additional infostealer functionality. The offer covered not just the source code but an entire attack capability maintained and sold as a package.

The price fight

In a comparative analysis of DDoS pricing over time, two patterns stood out. First, much of the market appears relatively consistent: about 64% of the services in our dataset maintained the same prices for long periods, in some cases for more than a decade. Second, the remaining 36% showed unpredictable fluctuations. For example, we discovered an actor whose prices were cut by 50% in just 20 days.

From a market perspective, this points to a trade that is stable in some areas but far from uniform.



The stability becomes weaker when we shift focus from the market in general to distinct actors. The example above tracks the prices advertised by a single provider for attacks of a day, week, and month duration over time. Instead of a consistent pattern, the figure shows unpredictable rises and falls. The most eye-catching case appears on October 2024, when the same actor advertised two drastically different prices on different forums. More than anything else, this highlights how actors adapt prices depending on the target audience.

Survival in the trade

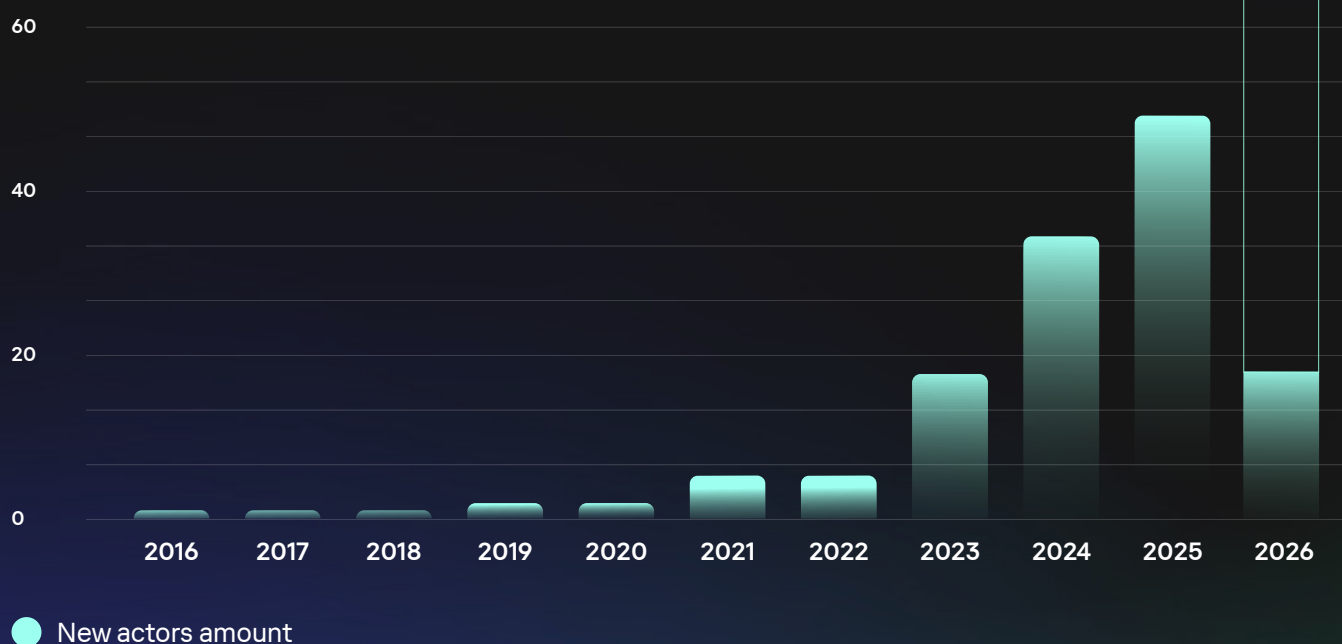
Born, sold, gone

Among the 148 actors that were active at some point in 2024 or earlier, the average lifetime (time between first and last advertisement of DDoS capability) is about 2.5 years, while the oldest among still-active providers marked 10 years of operation last year.

The number of newly appearing actors stayed relatively low until 2022. The first noticeable increase came in 2023, and the upward trend has continued since then. In the first quarter of 2026 alone, we have discovered 16 new actors. If the trend persists, the number of fresh actors in the market in 2026 may exceed the 2025 figure by at least 25%.

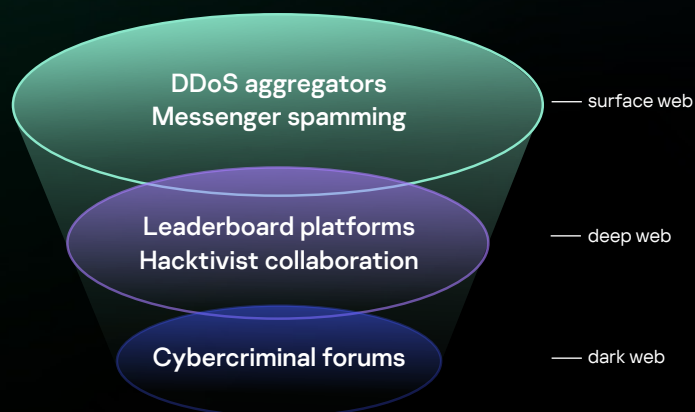
This growth likely reflects several things at once. DDoS attacks have become more popular overall, especially in recent years. Geopolitical tensions have fueled hacktivist groups to launch more frequent campaigns, making DDoS a more common type of attack. At the same time, open-source stresser tools have lowered the barrier to entry.

Distribution of new actors within the last decade
(including 2026 forecast)



Battles for attention

Visibility matters as much as capability in this market. A resource provider that cannot be found or remembered has little chances of acquiring customers, no matter what attack methods they claim to offer. To stay visible, DDoS actors promote themselves across several layers of the web, from DDoS aggregators to private cybercriminal forums.



These platforms do not serve the same purpose. Some are built for services comparison, while others rely on spam or reputation. Taken together, they form an advertising landscape, where actors compete for visibility.

Alongside these more familiar channels, we identified a newer and more distinct advertising mechanism: leaderboard platforms. Because they differ from ordinary promotion channels in both form and function, they are discussed separately in [The dark leaderboard](#) section.

DDoS aggregators

These are websites that gather multiple DDoS services in one place. They rank providers by “trust level”, user feedback and claimed attack layers. This way, they turn underground services into searchable catalogs.

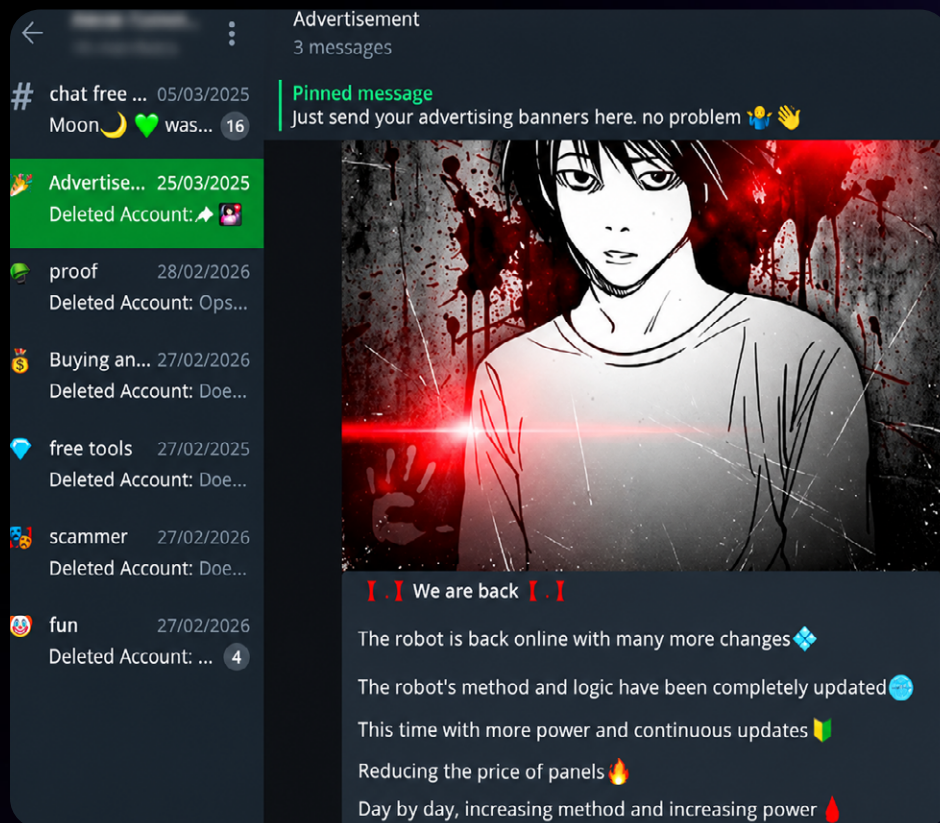
rank	Website	Description	Owner	Free	Layers	API	Status	Payments
#1	TheDarkVR	It's now time to trust the real pros	N/A	✓ Yes	3,4,7	✓ Yes	Hot	2 accepted PayPal
#2	TheDarkVR	TheDarkVR: Premium IP Stresser since 2002! Layer 4&7 Bypass Methods, High Power Per Each Slot!	McRobot9	✓ Yes	3,4,7	✓ Yes	Hot	2 accepted PayPal
#3	TheDarkVR	Bypass Methods (OVH, OAME, NFO)	N/A	✓ Yes	3,4,7	✓ Yes	Hot	1 accepted Crypto
#4	TheDarkVR	Private L7 Stresser, Cloudflare Bypass, 24h Duration * Zero logs * Dedicated Slots * API Access	N/A	✗ No	3,4,7	✓ Yes	Hot	1 accepted Crypto
#5	TheDarkVR	The most advanced IP stresser and network testing platform with both free and premium options.	N/A	✗ No	3,4,7	✓ Yes	Premium	1 accepted Crypto

Example of a DDoS aggregator website

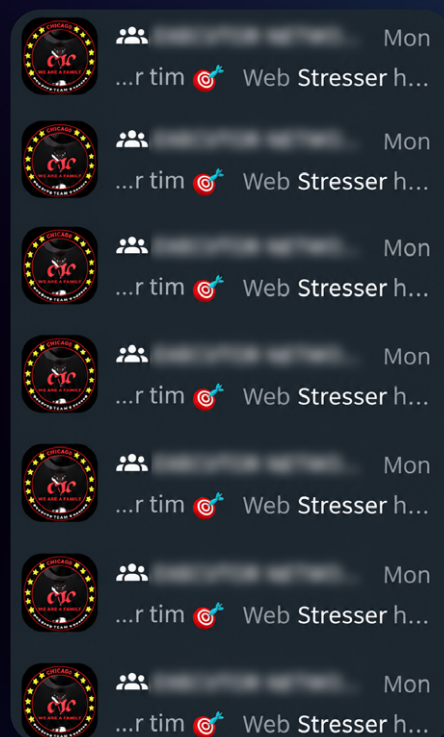
Messenger spamming

Another common route is direct promotion through messaging platforms. Here, actors advertise by posting repeated messages to one or several channels, often trying to catch attention through volume rather than credibility.

In some cases, channel administrators create dedicated threads for advertisements so that spam does not interrupt the general discussion.



Example of a dedicated advertisement topic

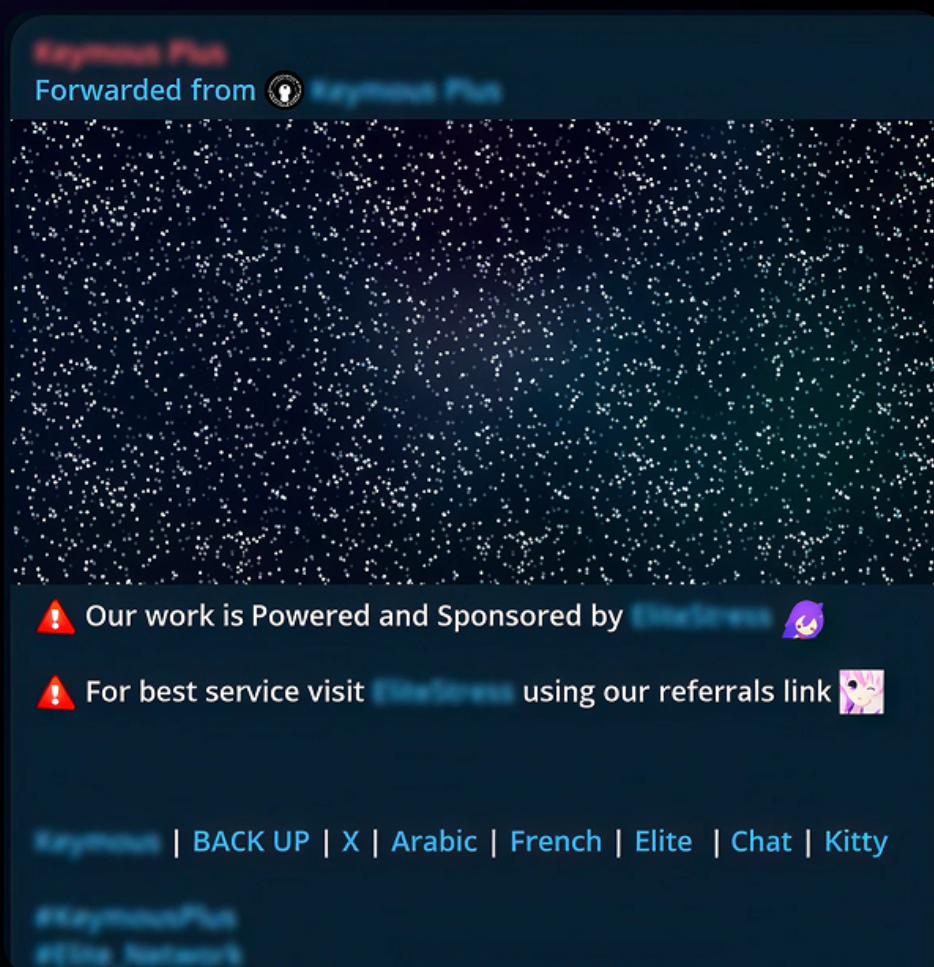


Example of a messenger spamming promotion

Hacktivist collaboration

Hacktivist groups don't only recruit people for ideologically motivated attacks. In some cases, they create alliances with DDoS resource providers to add external capability to their own campaigns. More capable groups have enough resources to build their own infrastructure. At least four active hacktivist groups promoted self-made DDoS tools.

For providers, these alliances serve their promotional purpose as well. Hacktivist channels are used as public proof of capability: attacks are announced, results are shared, and the provider gains visibility through association with an active campaign. In our dataset, nine providers showed hacktivist affiliation.

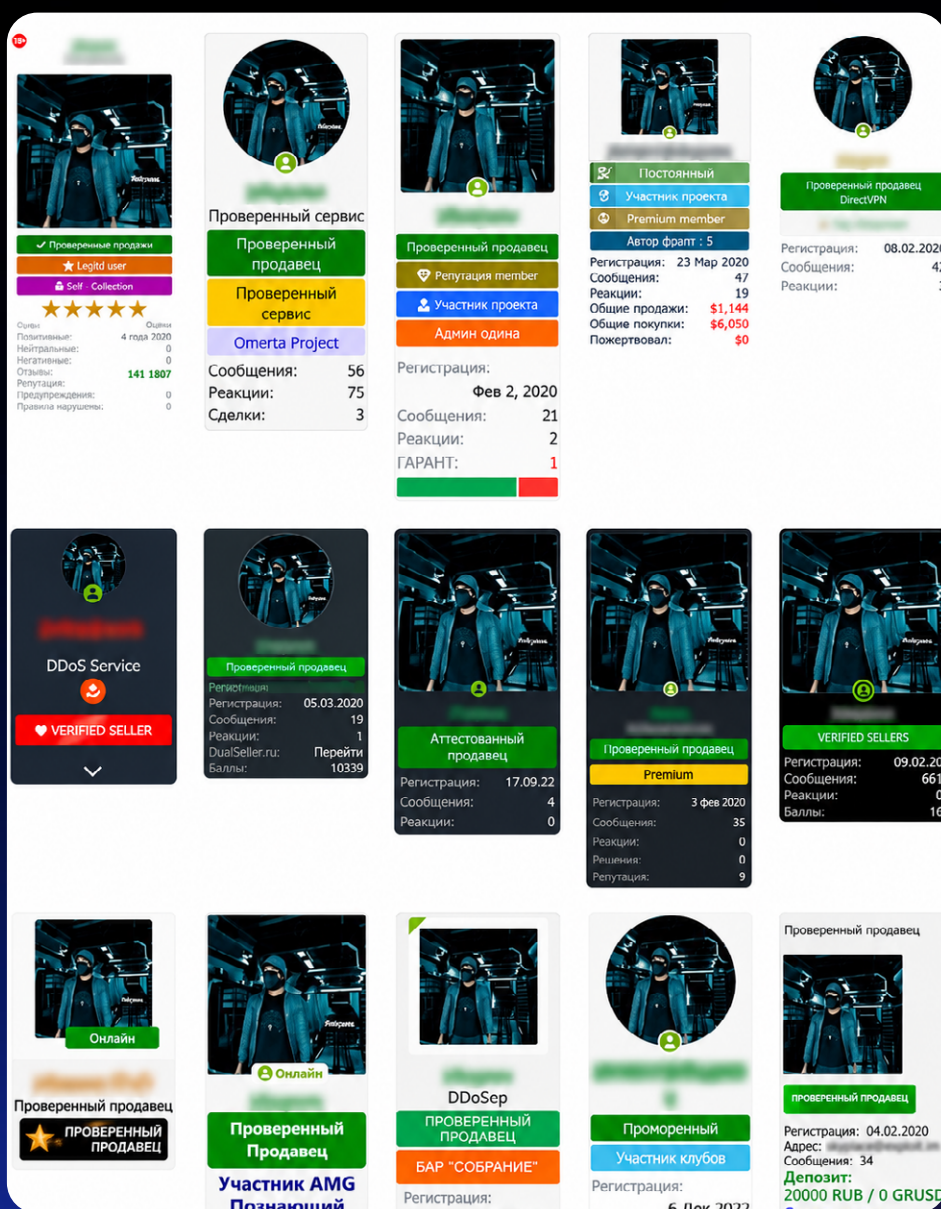


Example of an alliance statement between hacktivists and a stresser service

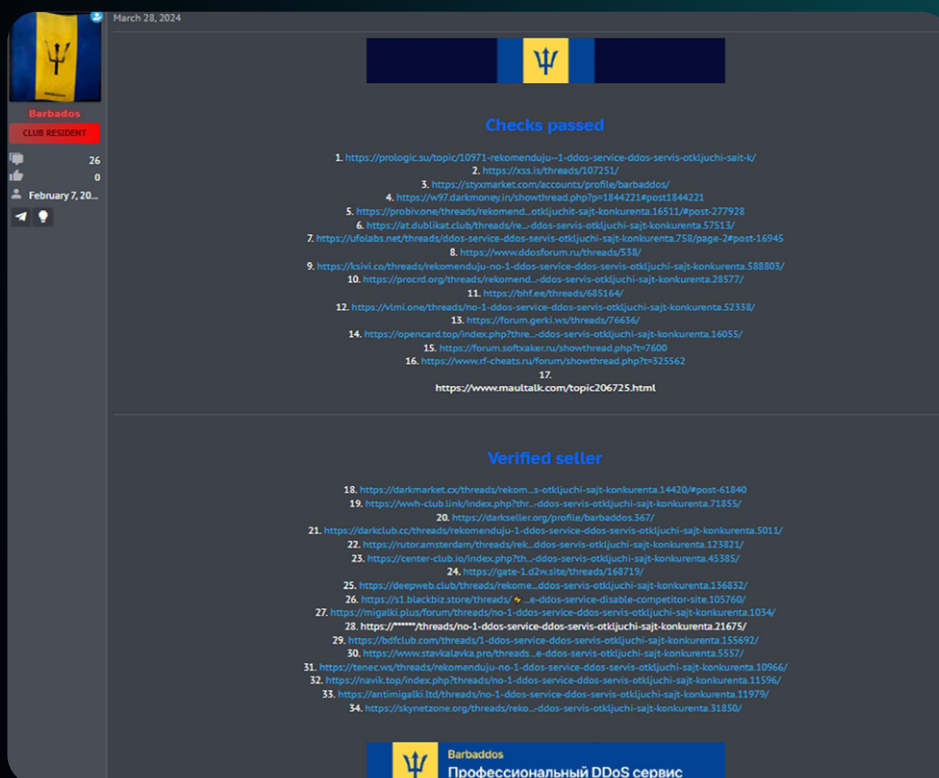
Cybercriminal forums

Cybercriminal forums remain one of the most established spaces for DDoS promotion. Several specialized forums present themselves as places to discuss DDoS protection technologies, yet the evidence suggests that they also serve as advertising space for attack providers. More general cybercriminal forums, not specializing in a single theme, often contain dedicated sections for DDoS-related promotions.

In this context, a forum reputation system becomes a part of a sales pitch. Many actors advertise on multiple forums at once, explicitly sharing links to other platforms to do both: reinforce their reputation or satisfy a forum's anti-scammer checks.



Example of an actor profile on different forums



Example of actor accounts on different forums

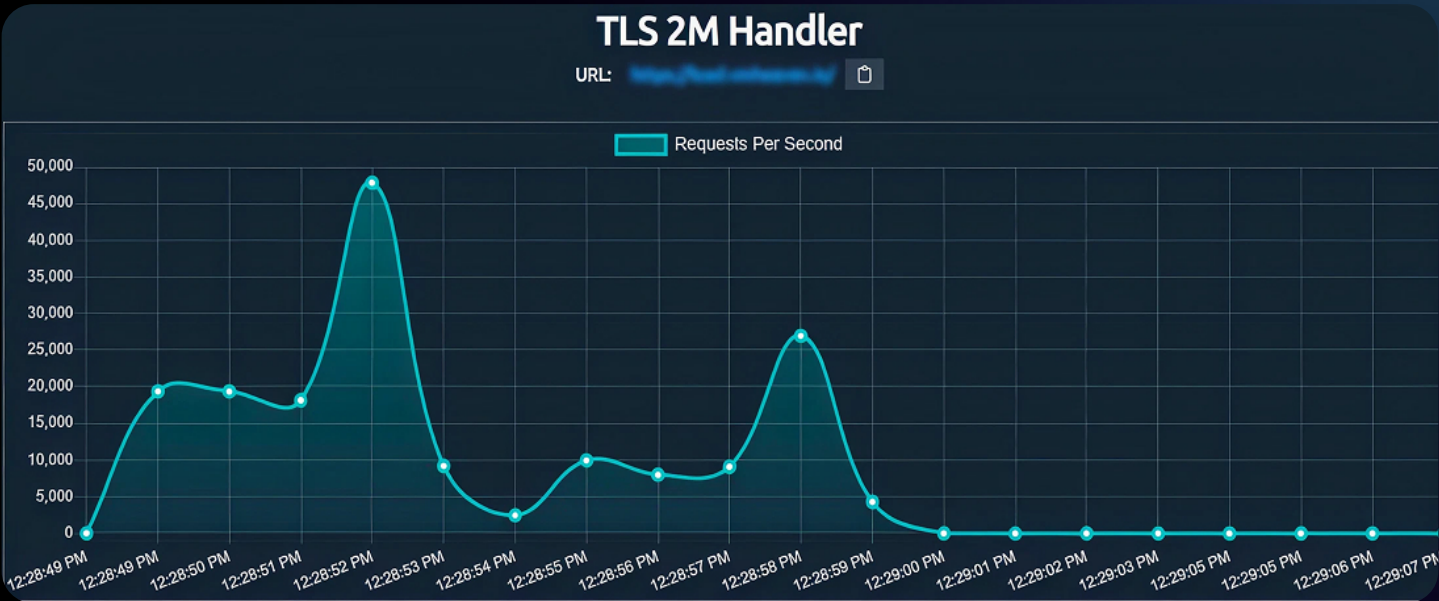
The leaderboard effect

Some actors don't consider typical advertisement channels at all. Instead, they use dedicated websites or Telegram bots that turn their attack capability into something measurable and tangible. Such systems are often referred to as DSTAT, borrowing the name from the system monitoring tool. This tool is deployed on servers, operated by DDoS providers or created specifically for ranking activity. A website or Telegram bot serves as an interface for attack monitoring and user ranking.

A participant interacts with the bot/website, chooses servers and attack methods, receives a target URL and launches an attack on it. During the measurement time, the bot/website records traffic characteristics such as requests per second or Gbps. Afterwards, the result is added to a public leaderboard under the participant's name.

	Website	Telegram bot
Typical name	dstat.*	*Count*
Live attack chart	Yes	No
Attack layer selection	Yes	Yes
Method selection	Yes	Yes
Can be used anonymously	Yes	No, by default
Ease of access	Lower	Higher

The point is not limited to measurement alone. These leaderboards claim public status. They give actors a way to compare power, compete for visibility, and advertise their services in the same space. In some chats, this logic is exaggerated: groups run long-term competitions and offer prizes to actors who stay in the top position for six months in a row.



Example of a chart on a leaderboard website

Count

Count

Layer4 Dstat

Pilih Server

Layer4 Dstat #1

Dstat Result

Peak Gbps: 0.05

Peak PPS: 25954

Time Period

Duration: 120s

Start Time: 2025-12-19 09:59:24 Jakarta

End Time: 2025-12-19 10:01:24 Jakarta

Example of an attack record in Telegram bot

/home

Layer4 Dstat #1

Rank Type All Time Ranking

Time 2026-03-24

16:26

Ohywv	28.25 Gbps
Xor	27.95 Gbps
Skid	27.19 Gbps
olivia [#relay]	27.17 Gbps
Kazi	26.56 Gbps
Daddys	26.17 Gbps
3ak	26.16 Gbps
phobosdev0	26.12 Gbps
liesha猎杀 国内1T/CC/私服/网站	26.08 Gbps
Adam	25.66 Gbps

Daily

7 Days

All Time

Back

Example of a leaderboard in Telegram bot

Beyond the DDoS

DDoS capability rarely exists in isolation. The same infrastructure used to generate a large volume of traffic and the same knowledge used to bypass protections, can be reused for different malicious activities. In our dataset, 43% of resource providers who advertised on cybercriminal forums also promoted side services.

We split these side services into two broad groups. The first, asset reuse, includes infrastructure, malware, and attack instruments repurposed for adjacent services. The second, knowledge reuse, is about turning experience to defensive offers, consulting, and training.

Assets



Mass abuse

- caller ID spoofing
- mail spam
- account bans/mass reporting
- website blacklisting
- domain takedown claims

33%



Instruments

- stealer botnets
- VPS rental
- script or botnet sales
- DDoS exploit sales

38%

Tradecraft



- Anti-DDoS services
- DDoS training

19%

Some of these side activities are close to DDoS itself, such as script sales, VPS rental or anti-DDoS services. Others apply the same infrastructure or operational logic to adjacent abuse models, from spam campaigns to mass reporting and takedown claims.

Evolving destructive power

To stay competitive, resource providers keep changing the attacks they offer. In our dataset, actors consistently favored **proprietary DDoS methods** over public tools. Open-source scripts remain available but actors rely on custom solutions to deliver stronger attacks and increase their chances of bypassing anti-DDoS protection.

This development includes customized traffic amplification, more advanced request handling, and adaptive evasion techniques designed to look like legitimate traffic. Some actors also referred to exploiting known **DoS weaknesses** or **mimicking real browser behavior** to get through defensive controls.

Competitive pressure is visible in advertisements, 33% of actors explicitly claimed the ability to bypass anti-DDoS protections. Across these claims, we identified 32 anti-DDoS vendors, covering L4, L7, and game server protection. Far fewer actors also mentioned AI-driven techniques for bypassing CAPTCHA challenges.

AI Powered DDoS service

Run realistic AI-driven stress tests in minutes. Simulate up to 700+ Gbit/s of traffic, find bottlenecks and keep your network online under any load.

[Get Started →](#) [Contact us](#)

Trusted by the world's biggest brands

 **TESTNOCSSA Method Update**

 What's new:

 Multi Targets added for panel users

 **Text Captcha DDoS-Guard bypass: our AI now solves it with 95% accuracy**

 Stay tuned for updates!

 Best regards, [https://h4ge.com](#)

 Current domain & admin contact: [https://h4ge.com](#)

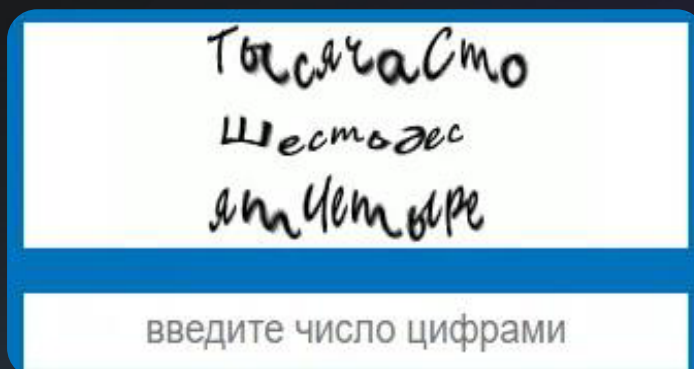
Examples of advertisements with AI-driven methods

Rules of engagement

Most providers in our dataset did not specify any target restrictions. Nonetheless, a smaller subset did set clear boundaries for who or what they were willing to attack. These restrictions were usually technical, but in some cases they also reflected particular preferences.

The observed restrictions fall into several groups:

- TLD-based restrictions: targets on domains `*.org`, `*.gov`, `*.edu`, and `*.med`.
- Technically inefficient web targets: `*.r2` web domains and `static websites`, which require disproportionately high traffic.
- Specific anti-DDoS protections: targets protected by `cyrillic CAPTCHAs` which are hardly deciphered by AI services.
- Service-category based: especially game servers and `*.onion` resources.
- Service function: for example, `large institutions and banks`.



Examples of cyrillic CAPTCHA

These boundaries suggest that even in a market built around disruption, not every target is equally desirable. In some cases the choice is more practical: some services are harder or less profitable to attack.

At the same time, geography rarely appears to be a serious constraint. Providers often emphasize that they can target systems worldwide.



In an example advertisement from our dataset, an actor explicitly mentioned its global reach. It is explained by the use of a diverse proxy pool, which helps to bypass geo-blocking measures used by anti-DDoS providers.

Summary

DDoS has evolved beyond a standalone attack technique into a well-established cybercriminal industry.

Accessibility continues to be one of the main factors driving this market's growth, reducing the barrier to entry for both inexperienced and highly skilled threat actors. Today, DDoS services are distributed through **brokered operations**, **stresser platforms**, and a **Telegram-based infrastructure** that has been gaining popularity since 2022.



Telegram
DDoS bots

- **27%** of DDoSaaS
- market is moving from websites to Telegram interfaces

DDoS attacks are carried out by a range of actors with different purposes: from ransomware operators and hacktivists to opportunistic individuals acting for personal gain.



DDoS attacks can affect any size organization in any sector

Service price range

\$1–\$30,000

The expansion of the market is noticeable when analyzing the number of newly appearing actors, which has been increasing since 2023. The possible causes of this growth are the geopolitical tensions that have fueled hacktivist groups to launch more frequent campaigns, and the popularity of open-source stresser tools which have lowered the barrier to entry.

DDoS infrastructure is expanding into adjacent cybercriminal operations: **43%** of providers also advertised side services as DDoS exploit sales, script and botnet sales, mass reporting and spamming, “DDoS protection services” and others. Competitive pressure is now driving **rapid technical adaptation**, particularly in bypass capabilities, specifically crafted methods of attack, and attack power.

23%

of actors advertised the capability of attacking games with specific crafted packages

36%

of actors claimed Tbps-scale attacks

33%

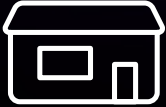
of actors claimed anti-DDoS bypass functionality

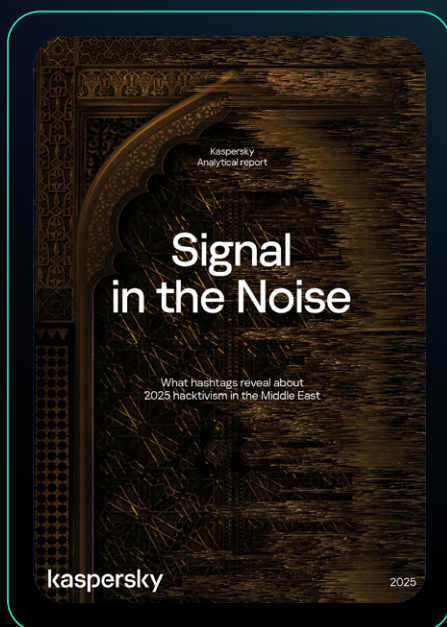
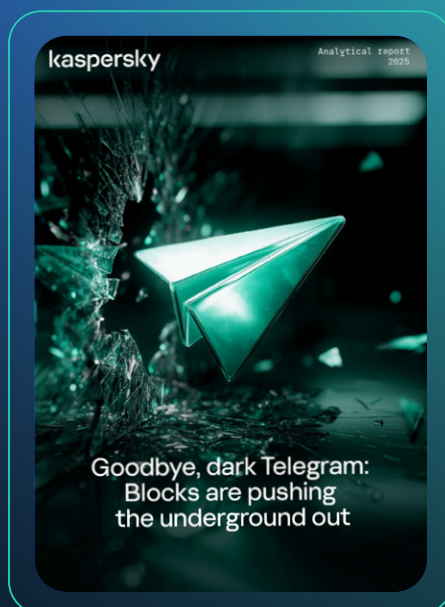
Emerging use of **AI-assisted CAPTCHA bypassing** and **browser-emulation techniques**



The DDoS market developed a well-established cybercriminal ecosystem supported by subscription models, automation, global accessibility, and continuous technical evolution.

Recommendations

Complexity of implementation	Run controlled DDoS simulations	Use stress testing or chaos engineering to validate defenses regularly, especially given the low cost and broad availability of DDoS services	
	Deploy multi-layer DDoS protection	Modern attacks target not only bandwidth at L3/L4, but also CPU and memory through crafted L7 requests	
	Track botnet intelligence and enrich detections with IoCs	Use known infrastructure, indicators, and actor information to detect and block malicious activity faster	
	Implement automated detection and response	As DDoS attacks unfold quickly and generate large amounts of telemetry, automation is essential for timely mitigation	
	Use a CDN and reverse proxy	Traffic distribution, origin shielding, and removal of single points of failure are key to resisting DDoS attacks	
	Separate critical services and enable autoscaling	Isolate critical functions from the rest of the infrastructure and scale them quickly when demand spikes	



Additional reports are available
on our website

[Learn more](#)

kaspersky

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

www.kaspersky.com