

# Low Orbit Ion Cannon

## LOIC

If you don't understand the meanings of the options you probably should NOT use this tool OR check the [Quick-Connect Guide!](#) Besides the obvious and topics covered in the other sections there are however some things to point out:

### The Target

Unless you know exactly what you are doing, you should use the "URL" field with the DNS of the server.

In 99.99% you do NOT want to target the IP!

Whatever you do - hit "Lock ON" BEFORE you start.

### Attack Options

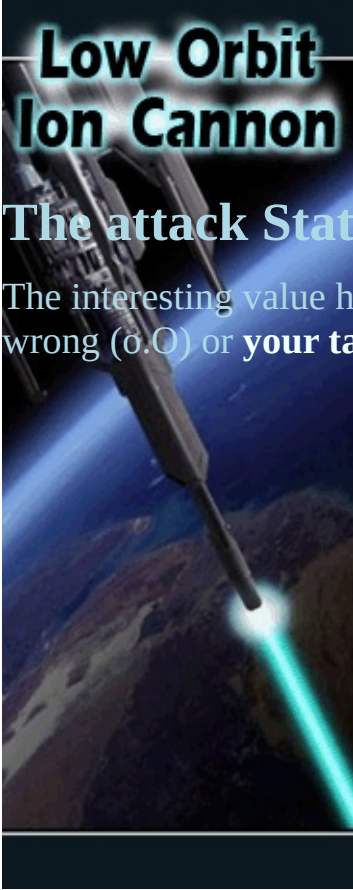
Choose an attack method from the pulldown and see which fields get enabled. You can change the speed slider on the right during the attack.

If you use ReCoil or slowLOIC you can change the amount of threads during the attack as well.

# Low Orbit Ion Cannon

## The attack Status

The interesting value here is "*Failed*"! If this goes up you are doing it epically wrong (o.O) or your target is **DOWN == EPIC WIN!**



# How to Laz0r for Newfags

## **Hello comrade!**

You have decided to provide your Laz0r to an OP for great justice and more lulz. Because you are a newfag the ubertrollz in the missioncontrol provided you with either an IRC-address or an URL to hand your helm over to the HiveMind.

## Connect to the HiveMind IRC

Put the address of the irc-server in the field labeled with "IRC server" at the top. In most cases you don't need to change the standard port or the channel. Select **"FUCKING HIVE MIND"** and you are done!

Right to the irc-options is the current status of your HiveMind connection, if it says *"Controlled by topic"*, *"Waiting"* or *"Connected"* you are all set.

## Use OverLord

If your OP has no IRC-Channel or gets constantly b& and is moving a lot, MC will most likely provide you with an URL for OverLord. Put this URL in the field under the IRC server right next to "**Damn OverLord**". Hopefully the ubertrollz told you if you should check "Up?" or not - if not leave it as is. In the field "Interval:" you can specify (in minutes) how often this is rechecked.

If the status on the right says: "*Done! Waiting for next Update..*" you are all set!

Please check out the [switches section](#) and the [basic GUI explanation](#).



# Low Orbit Ion Cannon

## Commandline Switches

*/hidden* - makes no sense without hivemind as well!  
*/hivemind irc.server.address 1234 #secret*

### Tips

maybe there comes more!?



## EZ Grab

Just fill out your attack-options .. run a short test and hit **F10!** paste that in the topic - done!



## boring Nerd-Stuff

First of all you need to have op-rights in the channel .. otherwise nobody listens to you directly .. at least you have to be able to change the topic.

Each command has to start with *!lazor*. If you want the attack to start append *start* to it .. *stop* to end the attack.

*default* set's the default values - use default as the the first command right after "*!lazor*" otherwise you end up resetting your own commands.

The commands available are: *targetip=* leave this as is (blank) unless you want to target a specific IP!

*targethost=*, *timeout=* (in seconds for 1.1.2.0+ // in milliseconds for 1.1.1.9 and previous versions!)

*subsite=*, *message=* both need to be URL-encoded

*port=*, *method=* {TCP|UDP|HTTP|ReCoil|slowLOIC}, *threads=*, *speed=* {0..50}

*wait=*, *random=*, *useget=*, *usegzip=* all {true|false}

## Tip

For backwards compability specify the ReCoil and SlowLOIC attack as follows:

*method=TCP method=ReCoil*

Due to the change of the timeout it might be best to go with the default values!

# OverLord - the WEB-LOIC

OverLord encodes the commands in Hyperlinks. You can place your commands virtually on any place in the internet. You can use Twitter, Facebook, any Forum / Message-Board / Blog or what so ever.

It is fully compatible with all common URL-shorteners and works with any header-redirector (the Location-Header is processed).

Most services give you the possibility to change the URL if you have signed up - this gives you the possibility to hand out one single link and control your PA by changing that link for new commands. In addition most services provide you with some "click-stats" which should give you an estimation of the size of your PA. (though not that exact .. there might be actual browsers trying to follow these links xD)

In addition OverLord lets you announce new HiveMind-IRC-Servers and even set countdowns for raids!

The countdown option let's you even set a time and give your fellow Anons time to report in WITHOUT revealing the target. the given URL is rechecked directly before the attack was scheduled to start, so that you set the actual target right before the attack starts by changing the command in the URL.

Besides command links OverLord supports backup-mirrors (as many as you want) - these mirrors can point to other mirros or contain target-links and so on.

## EZ Grab

Just fill out your attack-options .. run a short test and hit **F10!**

You can use any URL shortener you like or just choose one of the given services and click "**Make tiny**"

## boring Nerd-Stuff

All commands which are not set will be set to default automatically on the client!

There are 3 Methods:

I. Plain-Text Links: can ONLY specify TARGETS

*[LOIC: {OL-URI}]*

II: a-href Links:

II.a: Back-Up Mirrors - they contain no target information and point to sites, where target are posted.

*class="LO bu" href="{URI}"* - read diretion top to bottom

*class="LO bu r" href="{URI}"* - read direcion bottom to top

The read direction depends on the site: e.g. for twitter, where the newest post is on the top, you want to scan the site top-to-bottom for targets.

On Blogs / Boards where the newest posts are at the bottom, you want to scan in the reverse direction.

In the GUI the checkbox "Up?" scans top-to-bottom if checked and reverse otherwise.

The scan stops at the first encountered target and uses this as the current target - all BackUp Mirrors up to this point are stored. (mirrors after the 1st target in read-direction are ignored)

II.b: Target-Links

*class="LO tar" href="{OL-URI}"*

III. Plain Text instruction (this is depreciated) *[LOIC]*

*{command}:{value}*

*{command}:{value}*

*...*

*[/LOIC]*

If there is a "lot" of html-code merged into the text it is best to use the "@"-Delimiter:

[LOIC]{command}:{value}@<html goes here&tt;@{command}:{value}@.....  
[/LOIC]

### The URI-Syntax for Targets:

{OL-URI} = {URI}@{command}={value}@{single\_sign}@{command}=  
{value}@...

**IT IS HIGHLY RECOMMENDED TO USE URL-SHORTENER FOR THE  
TARGET-COMMANDS!!**

### Commands:

(there are 2 new commands - the others are the same as on IRC)

*targetip, targethost, timeout, subsite, message, port, method, threads, wait,  
random, speed, sockspthread, useget, usegzip*

*hivemind* - let's you set an Hive-Mind-Server over OverLord:

*@hivemind=irc.cooldomin.heros:6667#hivemind@*

If this command is used the control is immediately transferred to the HiveMind!  
(aka: OverLord STOPS working!) Therefore the hivemind command is best used  
alone without other commands.

*time* - you can set a timer for the beginning of the fun: *@time=YYYY/MM/DD  
HH:mm@* (time-zone is **UTC** for the time - the time-zone-correction is done by  
the client according to the system-settings and time!)

If a time command is issued the current attack stops and the Lazor waits until the  
time is reached. The target-information is updated once again EXACTLY at the  
beginning of the attack.

Using this it is possible, to set a time for all "connected" lazors WITHOUT  
revealing the target:

1. *http://hive.mind/go.hp?@time=2010/05/23 15:00@*

at 14:55 (UTC) you just change the Link to: *http://hive.mind/go.hp?*

*@time=2010/05/23 15:00@&@targetip=127.0.0.1@*

### **... enough with the crap - a real world example:**

On site <http://main.com> is the command center where you don't want to post  
target-information:

put somewhere on your site (in a .php / .txt / .html / .js or whatever file you  
have) the Back-Up-Mirrors for your OP:

```
<a class="LO bu" href="http://somefree-  
hoster.com/url/yourbackup">&nbsp;</a>  
<a class="LO bu" href="http://twitter.com/account">&nbsp;</a>  
<a class="LO bu r" href="http://xyx.chan.com/b/1234">&nbsp;</a>  
<a class="LO bu" href="http://bit.ly">&nbsp;</a>
```

As soon as one mirror fails the next is taken - the mirrors are accumulated at the client - so you can change them or add more after the majority of the nodes have read them once. Back-Up-Mirrors are only removed from the client, if one seems to be offline. (the effects of the Stress-Test on the client machine is (to some degree) mitigated!)

it might be a good idea, to hide the "LO"-Class with a (inline-) CSS or put it into any hidden container ... or just leave as is.

## ATTENTION: Backup Mirrors + Targets in one Page!

Pay attention to the scan-direction! If you read top-to-bottom (Up? = checked in the GUI) you HAVE TO PUT your mirrors BEFORE the first target-link!  
If you scan reverse you have to put the mirrors BELOW the target!

example: Scanning REVERSE + Mixed-Mode

<html-code>

<p>your very long paragraph LOIC: <http://bit.ly/abcde> your paragraph continues on for hours</p>

<more html>

<a style="display:none" class="LO bu" href="http://bit.ly">&nbsp;</a>

<footer-stuff>



## Tip

For backwards compability specify the ReCoil and SlowLOIC attack as follows:

`@method=TCP@&@method=ReCoil@`

Due to the change of the timeout it might be best to go with the default values!



## Options

In the "**message**" you can set some payload to send to the targeted service. If you need the newline chars, you can use `\r` and `\n` to construct the desired command / message.

If "**Append random chars**" is checked, 6 random characters are added at the end of the message.

"**Wait for reply**" waits until the packet is completely send. (you may want to check this on slower connections!)

## Remarks

"Failed" counts the unsuccessful connection attempts to the target. In most cases 10 threads is more than enough and should use all available upload-bandwidth, however with the speed-slider you can adjust this.



## Options

In the "**subsite**" you can specify the page to request.

If "**Append random chars**" is checked, 6 random characters are added at the end of the subsite. (usefull with dynamic pages and get-parameters)

If "**Wait for reply**" is checked, the complete document will be downloaded.

If it is unchecked, the page is only requested but not (completely) read. However the server starts to send the document until your receivebuffer is full. This option is especially intereseting for noncached dynamic pages where the processing time is more valuable than the used bandwidth.

In the "**Timeout**" field you set the read timeout in seconds. This is only important if "Wait for reply" is checked.

## Remarks

"Failed" counts the unsuccessful connection attempts to the target. If "Wait for reply" is checked, "Failed" is also increased, if the target took longer than the time specified in "Timeout" to deliver the page.

# ReCoil Attack

The ReCoil attack focuses on keeping the connections alive as long as possible, but it is not the same as [SlowLoris](#). It is more like a "reverse" DOS-attack.

A fully legit request is made but the download-speed is slowed down to nearly 0 by reading just enough from the network to keep the socket alive.

The attack itself produces NO errors - there are just a bunch of HTTP 200 in the access logs. If the server runs out of available resources and goes down, there might be an system error entry.

Especially all servers, that are vulnerable to SlowLoris, are vulnerable to this attack. ReCoil however is not as "easy" mitigated as SlowLoris. Think of it as a bunch of mobile devices requesting a page just before driving through a tunnel.



## Prerequisite

Due to the nature of the attack the requested site has to be at least 24kb (better larger).

The exact minimum filesize depends on the network buffer space of the attacking system. For most 10/100 connections around 24KB should work, while on gigabit connections filesizes beyond 64KB are needed.

NOTE: Your LOCAL link speed is the essential key not your internet speed! (meaning if you have a 1MBit internet connection and you are have a 1 gigabit link to your modem / router, you are pretty much screwed! --> target pdfs or big stuff like that!)

## Options

In the "**subsite**" you can specify the page to request. (keep the size in mind and do a bit scouting!)

If "**Append random chars**" is checked, 6 random characters are added at the end of the subsite. (usefull with dynamic pages and get-parameters)

If "**Wait for reply**" is checked, ReCoil follows Header redirects and discards early documents, which are smaller than 16KB. (Only apply this if needed)

The "**Timeout**" field is for the wait time in seconds between reading from each socket. This must be less than the write timeout on the target side.

The amount of worker "**threads**" can be changed during the attack at any time. This value should be initially lower than the maximum allowed half-open connections.

To consume even more memory you can additionally check the "**use gZip**" - but remember the resulting document has to be of reasonable size!

In the "**Sockets / Thread**" field you can define the number of connections per thread. (this number should not be insanely high - if you go over 100 it might be better to increase the amount of threads!)

the speed-slider sets just the delay between the creation of sockets.

## Remarks

The "requested" value shows the amount of currently connected sockets. If no thread is in the "Connecting" state you should increase the number of threads - if all your threads or most of them are connecting you should lower the amount of threads.

"Failed" counts the connections which were reset by the server. If "Wait for reply" is checked it also counts the unsuccessful attempts which are early discarded.

If "failed" goes up too fast you are doing it WRONG!

## Tip

If you target a system which is not vulnerable to this attack you can always go for port-starving!

Just use up all max possible 64K connections and you are done! (running 16 clients with 5.000 connections each should do the trick!)



## Options

In the "**subsite**" you can specify the page to request.

If "**Append random chars**" is checked, 6 random characters are added at the end of the subsite. (usefull with dynamic pages and get-parameters)

The "**Timeout**" field is for the wait time in seconds between sending a new part of the header. This must be less than the read timeout on the target side.

The amount of worker "**threads**" can be changed during the attack at any time. This value should be initially lower than the maximum allowed half-open connections.

Check "**use gZip**" to check for CEV-2009-1891.

Check "**use GET**" to use the GET-command instead of POST. (mods like http-ready mitigate GET-attacks)

In the "**Sockets / Thread**" field you can define the number of connections per thread. (this number should not be insanely high - if you go over 100 it might be better to increase the amount of threads!)

the speed-slider sets just the delay between the creation of sockets.

## Remarks

The "requested" value shows the amount of currently connected sockets. If no thread is in the "Connecting" state you should increase the number of threads - if all your threads or most of them are connecting you should lower the amount of threads.

"Failed" counts the connections which were reset by the server.

If "failed" goes up too fast you are doing it **WRONG!**

## Tip

If you target a system which is not vulnerable to this attack you can always go for port-starving!

Just use up all max possible 64K connections and you are done! (running 16 clients with 5.000 connections each should do the trick!)



# Low Orbit Ion Cannon



About L O I C

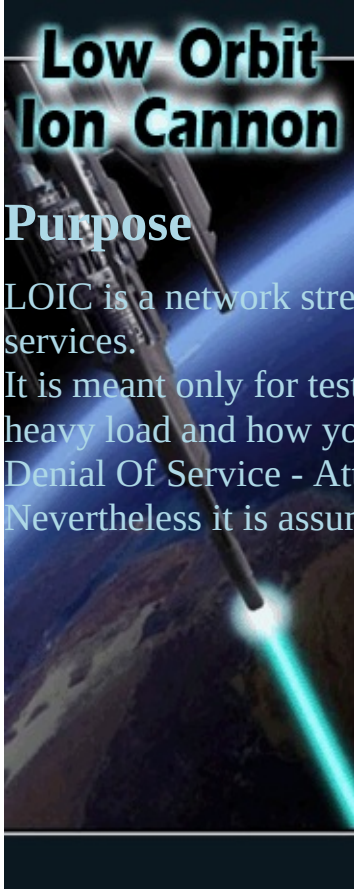
# Low Orbit Ion Cannon

## Purpose

LOIC is a network stress testing tool for simulating and testing peaks on various services.

It is meant only for testing how your servers cope with many requests and under heavy load and how your server does respond to several (D)DOS ((Distributed) Denial Of Service - Attacks).

Nevertheless it is assumed, that you own the servers you are testing!



# Low Orbit Ion Cannon

## License

Public Domain - Feel free to do what ever you want with this.



# Low Orbit Ion Cannon

## History

The first known to mankind version of LOIc was created by [Praetox on SF](#)  
[NewEraCracker](#) adopted it and added HiveMind to it and made some bugfixes /  
adoptions to the original source.

After version 1.1.1.9 [BeSquare](#) joined in and made some contributions.



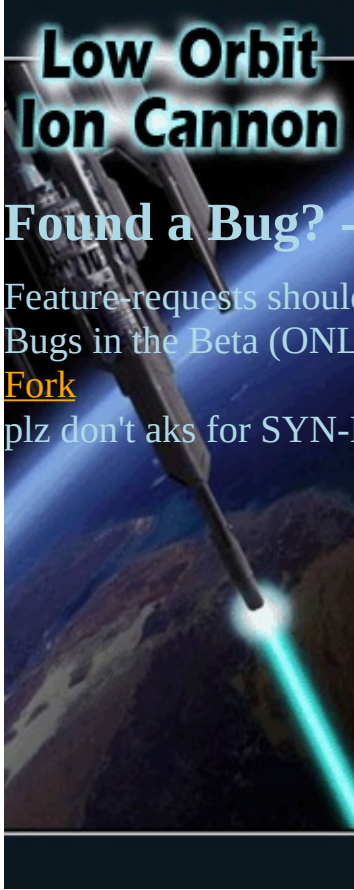
# Low Orbit Ion Cannon

## Found a Bug? - Can has Feature? - This Help suckx?

Feature-requests should be made in [NewEraCracker's Tracker](#)

Bugs in the Beta (ONLY the BETA!) or this Help can also reported at [BeSquare's Fork](#)

plz don't aks for SYN-Flooder! - that simply does NOT work on Windows!



# Low Orbit Ion Cannon

## Disclaimer

This tool is released for educational purposes only and comes with no warranty at all.

None of the authors or contributors can be held responsible for any action taken by the users of this tool!

