

IMPORTANTLY!

- Before starting any DDOS attack, you need to connect a VPN, which will need to be changed periodically (except for the use of proxy scripts)
- Try to use the most effective way
attacks (see Attack: the most effective way)
- Do not attack single targets, watch Telegram channels that attack others, and just join. So we have more chances to "put hostile sites back".
- Glory to Ukraine!
- Russian warship, go nah * y!

Content (clickable)

How to connect a VPN?	2
How to check if your IP address has changed	5
Attack: mega simple level	6
Attack: simple level	9
Attack: intermediate level	13
Attack: advanced level	15
Attack: The Most Effective Way	16
Checking the result of DDOS-attacks	17
Additional resources	18
Afterword	20

How to connect a VPN?

The easiest and most effective way is to use ready-made programs that can be downloaded to your computer and change with one button. its location.

If you know other ways to change the IP address, or configure the VPN, you you can use them, all ap tu yu.

The following is a list of such programs and links to them.

Just download, install, choose any country (in some cases it is advisable to use the IP-addresses of Russia, in some European or American IP, it all depends on the task).

I advise you to download 2-3 programs. Because it happens that one of the programs begins to fake.

Warning! I advise you to use Hotspot Shield as the main program to change your IP address, now it is the best choice.

1. ~~Hotspot Shield~~

Currently, there is a promotion for Ukrainians: Premium tariff for one month. Just register and download the program. If the promotion is no longer valid, then just choose the Premium tariff, subscribe for 1 month, connect a virtual card (you can with 0 balance) and use Premium

version for 1 week. Then do not forget to disable the card, so as not to write off the subscription fee.

+	-
Simple interface	
There is a month of Premium account for Ukrainians	
There are Russian IPs	
Does not lag	

2. [F-Secure Freedom](#)

Register here and download the Freedom program. Now it is available for free for Ukrainians for 30 days.

+	-
Simple interface No	No Russian IP
need to tie your own card	
Does not lag	

3. [Urban VPN](#)

Completely free. Option for those who do not want to steam for a long time VPN settings.

+	-
Simple interface	He can lie
Completely free	Russian IPs in most cases do not work
There are Russian IPs	

4. [ClearVPN](#)

Made a promo for Ukrainians (SAVEUKRAINE) with six months of free access. Because of this, most Ukrainians began to use it and it began to rise very much. So now I advise you to use others programs.

+	-
Simple interface There	Can lag very hard
is a promo code	Russian IPs do not work

5. [Windscribe](#)

Paid. And that's it. You can find free best alternatives. I do not recommend.

+	-
Simple interface	Paid
	Russian IPs do not work
	Can lag very hard

6. [KeepSolid VPN Unlimited](#)

Similar to ClearVPN. They did a promo for Ukrainians with a six-month subscription, which, unfortunately, I can't even find now (who wants to use this VPN - google it). Due to this, strong lags are possible. Not now

I recommend using this program.

+	-
Simple interface There	No Russian IP
is a promo code	Can lag very hard

How to check if your IP address has changed

Importantly! After you set up and run the VPN, you need to check whether your address has really changed (there are cases when the service fakes or changes the address to the wrong country that you chose).

Here is a link where you can check your current location:

- [Resource 1](#)
- [Resource 2](#)
- [Resource 3](#)

Attack: mega simple level

For those who do not want to bother at all, there is a list of sites and programs which can be easily opened and they themselves will carry out attacks on certain sites. Just follow the instructions described on the site itself, or in the program and forward.

Importantly! Don't forget about the enabled VPN, which needs to be changed from time to time.

As an alternative to VPN, you can download Tor Browser [at this link](#), after downloading it, open the tab with the sites listed below and enjoy the attacks on Russian sites. Each time you log in to the browser, your IP will change. ~~Download Tor Browser~~ programs from items 4 and 5.

1. [yyyyyyyyy.yyy](#)

Attacks a list of Russian sites that can be changed.

Warning! Be careful when opening this site your laptop or computer may hang out.

Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

2. <http://www.lookquizru.xyz/>

Attacks one of the sites that is relevant at the moment (the site for the attack is changing dynamically).

The site was developed by the KiberBULL team. [Links to their Telegrams channel.](#)

Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

3. <https://2022pollquizinru.xyz/>

Attacks the standard list of Russian sites.

Another site developed by the KiberBULL team. [Links to them](#)
[Telegram channel](#).

Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

4. <https://help-ukraine-win.com.ua>

Attacks a list of sites that change dynamically on their own using a proxy. All you have to do is install and run the program.

The program was developed by the UA Cyber SHIELD team. [Links to their Telegram channel](#). Follow the link, choose the language convenient for you, then the simplest level, follow the instructions, install the program and open it on your computer.

Importantly! Don't forget about the enabled VPN! Tor Browser here it is not advisable to use!

5. [DB1000N](#)

Similarly to the previous program attacks a certain list of sites that independently dynamically changes.

The program was developed by the DDOS team in the country of SEPARIV (Cyber-Cossacks). [Links to their Telegram channel](#). Just follow the instructions, install the program and open it on your computer.

Importantly! Don't forget about the enabled VPN! Tor Browser here it is not advisable to use!

6. <https://playforukraine.live/>

And they even created it! A game that can be played in the browser, and your every move attacks one of the Russian sites.

Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

7. <https://stop-russian-propaganda.pp.ua/>

Attacks the standard list of Russian sites.

Warning! Be careful when opening this site your laptop or computer may hang out.

Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

8. <https://ban-dera.com/>

Attacks the standard list of Russian sites.

Warning! Be careful when opening this site your laptop or computer may hang out.

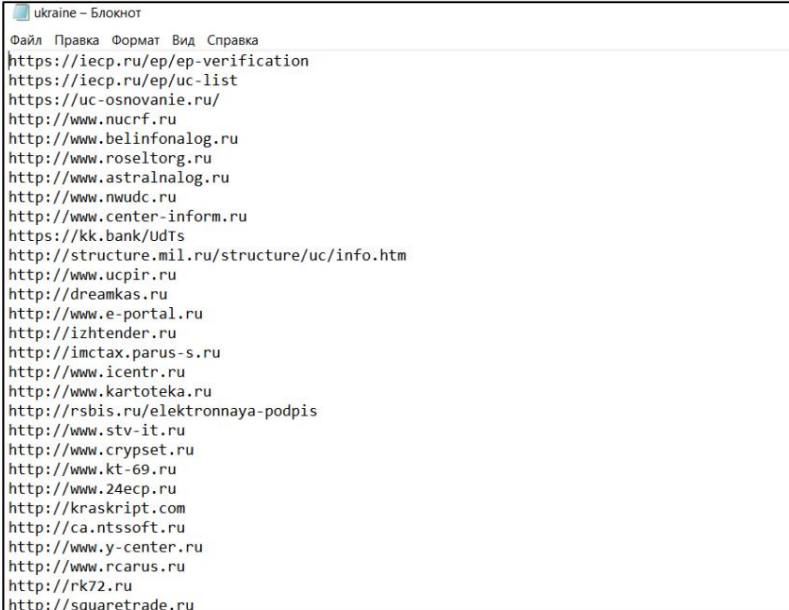
Importantly! Remember to turn on the VPN you need from time to time change, or Tor Browser, which you need to revisit from time to time!

Attack: simple level

For greater maneuver of personal actions of the attacker, you can use ready-made programs that are quite easy to use.

1. Hello World

- Use [this link to download this program](#).
- Next, download the archive and unzip it to the folder of the same name.
- Go inside the folder and in the file "ukraine.txt" just transfer the sites you want to attack (each site on a new line, an example in the screen below).



```
ukraine - Блокнот
Файл  Правка  Формат  Вид  Справка
https://iecp.ru/ep/ep-verification
https://iecp.ru/ep/uc-list
https://uc-osnovanie.ru/
http://www.nucrf.ru
http://www.belinfonolog.ru
http://www.roseltorg.ru
http://www.astralnalog.ru
http://www.nwudc.ru
http://www.center-inform.ru
https://kk.bank/UdTs
http://structure.mil.ru/structure/uc/info.htm
http://www.ucpir.ru
http://dreamkas.ru
http://www.e-portal.ru
http://izhtender.ru
http://imctax.parus-s.ru
http://www.icentr.ru
http://www.kartoteka.ru
http://rsbis.ru/elektronnaya-podpis
http://www.stv-it.ru
http://www.crypset.ru
http://www.kt-69.ru
http://www.24ecp.ru
http://kraskript.com
http://ca.ntssoft.ru
http://www.y-center.ru
http://www.rcarus.ru
http://rk72.ru
http://squaretrade.ru
```

- If in Windows, just run `pay_ukraine_windows.exe`, a separate window will open, as shown in the screen below, and enjoy the collapse of the Russian Federation

```
D:\Downloads\Hello World\pray_ukraine_windows.exe
loading http://rsbis.ru/elektronnaya-podpis
loading http://structure.mil.ru/structure/uc/info.htm
loading http://www.astralnalog.ru
loading http://www.belinfonalog.ru
loading http://www.icentr.ru
loading http://mascom-it.ru
loading http://epnow.ru
loading http://ucestp.ru
loading http://www.ucpir.ru
loading http://epnow.ru
loading http://elkursk.ru
loading https://iecp.ru/ep/ep-verification
loading http://www.center-inform.ru
loading http://www.ucpir.ru
loading http://www.nucrf.ru
```

- If you have Linux or MacOS, we do the following:
 - o open SystemPreference -> Security & Privacy -> Privacy -> Developer Tool -> Enable Terminal
 - o open the Terminal inside the folder where the file pray_ukraine_mac is located, or open the Terminal and just go to the folder where the file pray_ukraine_mac is located
 - o prescribe commands:
 - `chmod + x pray_ukraine_mac`
 - `sudo ./pray_ukraine_mac`
 - o enjoy the collapse of the Russian Federation

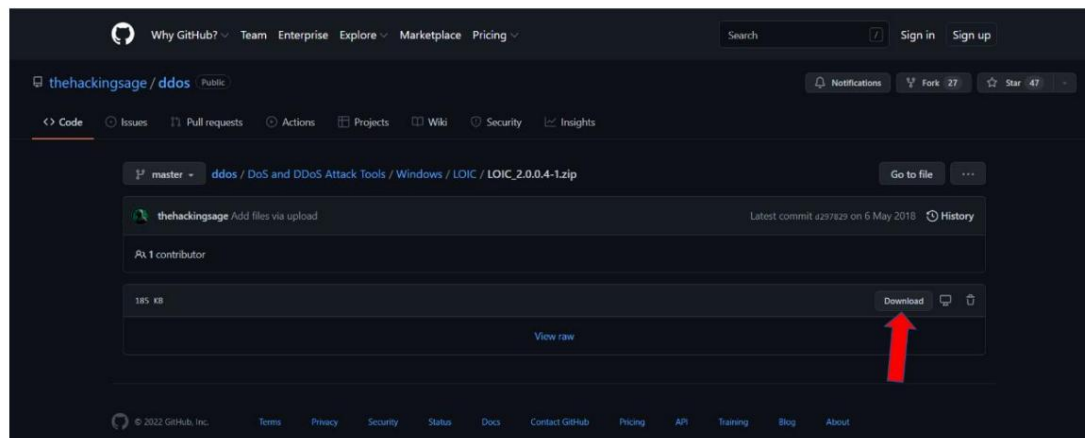
The program was developed by the Telegram channel Pogantsi (Fire show). [Links to their Telegram channel.](#)

Importantly! Don't forget about the enabled VPN, which needs to be changed from time to time.

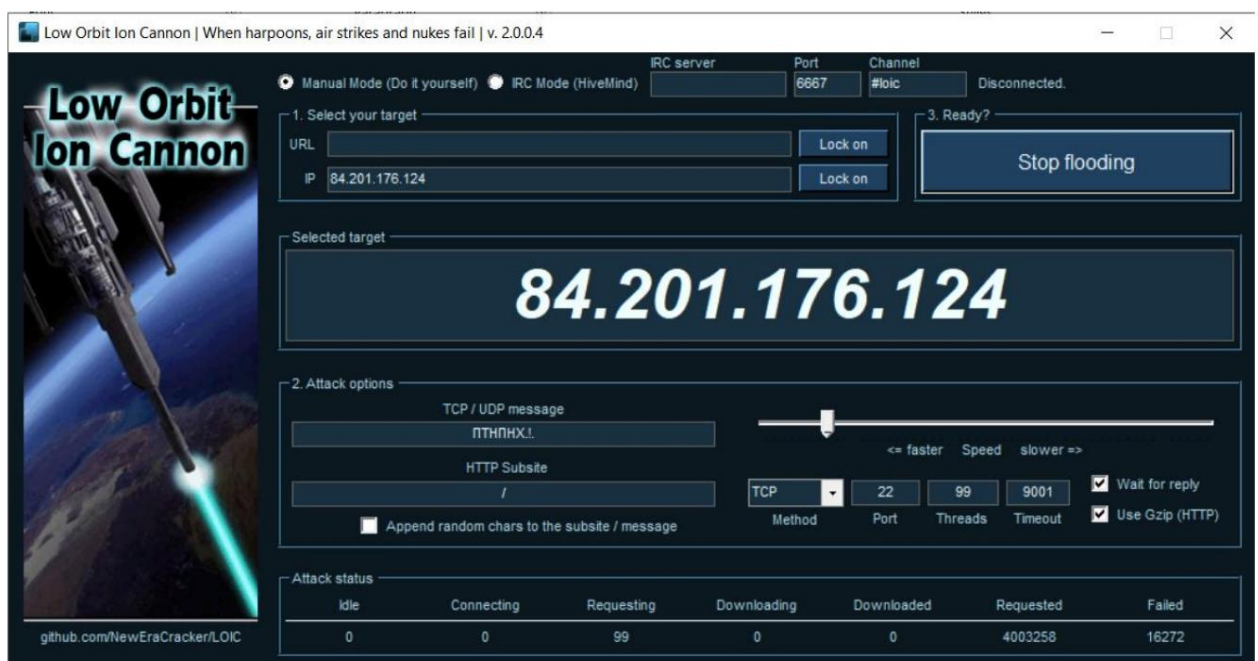
2. LOIC

Warning! For Windows users only!

- Use [this link](#) to download this program.



- It may be that your computer may block the download of this archive, so you can disable the antivirus (**at your own risk!**) While downloading and installing this program. However, after installation, be sure to enable antivirus, it would not have quarrel over this program.
- Unzip the archive to any separate folder.
- Inside it run the file LOIC.exe



- Next or in the URL field pass the physical address of the site we want to attack (for example, <https://interfax.ru/>) and click Lock on, or in the IP field pass the IP address of the site and click Lock on (as shown in the screen above).

- In the TCP / UDP message field, add any message you want. It is desirable want to bring to Russia to change it every time when you change your IP address.
- Set the Speed slider either to the left or a little closer to the center on the left (as shown in the screen above).
- Next, select Method (TCP, HTTP or UDP). In most Telegram channels that publish some targets for the attack, a specific method is already specified, then we just choose it.
- Next, select the port in the Port field (the field next to the Method field, not the one at the top, at the top of the Port we leave the default and equal to 6667). The port is what is indicated after the colon in the IP address, for example, for 84.201.176.124:22 port is the number 22. In most Telegram channels that publish some targets for the attack already specified specific port, then just choose it.
- **Important!** If Method and Port are not specified, try standard ports and methods for sites. For example, TCP and 443, TCP and 22, HTTP and 80, other options are possible.
- In the Threads field, select the maximum possible number that your computer allows without making a mistake. Start with 200, then 100 and so on. In my case, it's 99.
- All other fields are left unchanged.
- Press the IMMA CHARGIN MAH LAZER button and enjoy

the collapse of the Russian Federation

- How to understand that everything works? If the number of Requested increases and Failed appears (screen below), then you do it
That's right, keep it up.

Attack status						
Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
0	0	99	0	0	363332	525

Importantly! Remember to turn on the VPN you need from time to time change.

Attack: Intermediate

For those who understand how to install and run Docker, there are already many ready-made scripts that are fairly easy to run from a local or virtual cars.

[Here is a link](#) to a tutorial on how to install Docker on different operating systems and how to run a specific script on Docker.

Everything is written in the *DdoS Instructions*.

There are also other options in *Used Sources and Tutorials* on how to run scripts with DDOS attacks using other Docker containers, scripts written in Python and other programming languages.

This tutorial was compiled by the DDOS team for the country of SEPARS (Cyber Cossacks). [Links to their Telegram channel](#).

Also quite recently appeared Telegram channel Ukrainian Reaper, which mainly teaches guides on Docker and Python scripts. [Link to this Telegram channel](#). You can find all the necessary articles in the fixed messages of the channel. The following guides are currently available:

- [Preparing a virtual workspace for DDOS attacks](#)
- [DDoS Ripper Tutorial](#)
- [MHDDoS Tutorial](#)
- [Deep MHDDoS parsing](#)
- [Intelligence for DDOS attacks](#)
- [Proxychains attack from within the enemy's infrastructure](#)
- [Parse MHDDoS_proxy](#)
- [Proxy update for MHDDoS_proxy](#)

Importantly! First you need to disassemble [the first guide](#) that will allow you to deploy a virtual machine. Next, choose a script to your liking from the following guides.

Warning! At the moment, almost all the teams that publish in this Telegram channel Ukrainian Reaper ([link to this Telegram channel](#)) relate to the script described in the [last guide](#). I advise you to deal with it.

Importantly! Before running commands to attack a resource you can check the availability of this resource using the commands:

- `curl http://213.24.76.25:1935/tcp -I` (for IP)
- `curl https://scr.online.sberbank.ru/api/fl/idgib-w-3ds -I` (at)

Importantly! If you attack from a local machine, don't forget about the enabled VPN, which needs to be changed from time to time.

Attack: advanced level

With the help of Docker, Docker containers and other scripts on special services, you can deploy many virtual machines on which you can run a large number of DDOS-attacks.

The following are tutorials on how to deploy such virtual machines on AWS, Digital Ocean, Azure and Google Cloud.

- [DDOS on AWS](#)
- [DDOS on AWS 2](#)
- [DDOS on AWS \(videos\)](#) •
- [DDOS on Digital Ocean](#) •
- [DDOS on Digital Ocean 2](#) •
- [DDOS on Azure](#)
- [DDOS on Azure 2](#)
- [DDOS on Google Cloud](#) •
- [DDOS on Google Cloud \(video\)](#)

Attack: The most effective way

The DDOS Tutorial for all team has written two very useful guides to help you carry out attacks on enemy sites. I advise everyone who wants to attack effectively and effectively, deal with them, configure the machine and use the MHDDoS_proxy script according to the guide.

If you have any questions, ask them in the comments below any posts on [this Telegram channel](#).

- [How to deploy virtual machines to Digital Ocean](#)
- [Detailed analysis of MHDDoS_proxy](#)

The DDOS Tutorial for all team also has a HitHub repository, where the above guides are available and new ones will appear later.

- [Links to GitHub](#)

Check the result of DDOS attacks

Everyone who attacks would like to monitor the progress of their attacks, whether they make any sense at all and whether they work.

Below are two services where you can pass or physical address of the site (for example, <https://interfax.ru/>), or an IP address with a port (for example, 84.201.176.124:22).

- <https://port.ping.pe>
- <https://check-host.net/check-http>

There is also a site where you can use the IP address to find all the necessary information about this IP address, such as: open ports (see Port Scanner), or whether the site is pinged or not (see Ping):

- <https://viewdns.info/>

Warning! Also recently in the Telegram channel Ukrainian Reaper ([link to this Telegram channel](#)) came out a guide on how to properly prepare for DDOS attacks. I advise everyone to read and understand, there are many useful links:

- [Intelligence for DDOS attacks](#)

Additional resources

Telegram channels (DDOS related):

- [DDOS in the country of SEPARS \(Cyber-Cossacks\)](#) • [DDOS Tutorial for all](#)
- [ddos cats](#)
- [KiberBULL](#)
- [Ukrainian Reaper](#) • [Zion](#)
- [UA Cyber SHIELD](#)

Telegram channels (other):

- [IT ARMY of Ukraine](#) (Cyber Army of Ukraine) • [Anti-Putin Hackathon](#) (Various projects to defeat the occupier) • [DataLeaks](#) (Leaks from various Russian databases)

Telegram channels with constant information on how to remind the world community of Russia's attack:

- [UkrTvi Army](#) • [UkrInsta Army](#)

Useful GitHub repositories:

- [DDoS for all](#)
- [Original MHDDoS](#) • [MHDDoS_proxy](#) • [Ukrainian Reaper](#)
- [DB1000N](#)

[Resources for DDOS attacks](#)

Website with all the necessary information about Ukraine during the war:

<https://viyna.net/>

A useful site that allows you to quickly convert the goals given in the IT Army of Ukraine, in the format used for teams:

<https://ddosukraine.com.ua/>

Slack channel with various projects for people in the field of IT (in order to be moderated you need to have a working LinkedIn account):

[UA Tech Power](#)

Personal data of Russian users:

[IT ARMY Leaks](#)

Epilogue

- If you have any questions, please contact [this Telegram channel](#) and write them in the comments below the posts.
- Follow the [GitHub repository](#), we will add new guides.
- I would be very grateful for spreading the link to the Telegram channel DDOS Tutorial for all (https://t.me/+Z_LFYsLfmmM4YmUy), and for distributing this file with the Tutorial.

Warning!

- You choose whether to carry out attacks on Russian sites or not!
- The author of this manual is not responsible for its use instructions!
- Glory to Ukraine!
- Russian warship, go nah * y!