DISCLAIMER : This manual is strictly for educational purposes only. Please be aware that attacking (port scanning, DDOS, probing, PEN, etc) is highly illegal in many countries and if caught, you may be looking a prison time. Although I believe that the secret services of many countries will not pursue any contesters actively due to the extraordinary circumstances, they have every right to do so. It's YOU that is doing something illegal. Give yourself a few minutes to think it through before you decide to participate!

Okay, so you thought it through … excellent. Oh, one more thing .. No one in our groups is responsible if you get caught and you'll spend a few years picking up your soap for a bloke called bubba. Also, most of us don't have the time to teach someone how to operate an operating system or install a program, so we assume that you know a thing or two about Linux/*nix OS. If you insist on using Windows, there will be a separate entry for that soon. This tutorial is not about reinventing the wheel. If you click on links, there will be explained of how to install stuff. For the sake of speed, this is not included in this manual.

If you have a good addition to this document, please don't hesitate to DM the group admin. He/she will make sure that the information is added to the next document version.

Even when you're not comfortable with attacking targets, there are still (legal) things you can do to help us. Check the last section "Tips and Tricks" to see if there is anything that is suitable for you. We will update this document regularly with new information. You have a tip? .. grab an admin and he/she will make sure this document will be updated.

We suggest you start with this manual first and then if you're hungry for more information you can check out the IT Army of Ukraine website. There is a lot of information on that website that covers pretty much the same topics as this manual and in some cases a bit more. The website does have a few newcomers' tips but it is mainly written for people with some degree of IT knowledge. Nevertheless worthwhile checking out.

https://hackmd.io/pl_ucHTWQUmO9ubmzRT1tQ

Step 1 : Operating system

1.1 TAILS OS

Pick your OS, preferably a System V (POSIX complaint OS). I suggest you install TAILS, which is Debian based, for a number of reasons. First, it will hide your identity better than other OS and it will run off a USB stick. That means you can use your windows box to run it.

https://tails.boum.org/

Techrepublic also wrote a good article about TAILS, I suggest you read that, too :

https://www.techrepublic.com/article/getting-started-with-tails-the-encrypted-leave-no-trace-operating-system/

1.2 : ParrotOS

Parrot is a worldwide community of developers and security specialists that work together to build a shared framework of tools to make their job easier, standardized and more reliable and secure. Parrot OS, the flagship product of Parrot Security is a GNU/Linux distribution based on Debian and designed with Security and Privacy in mind. It includes a full portable laboratory for all kinds of cyber security operations, from pentesting to digital forensics and reverse engineering, but it also includes everything needed to develop your own software or keep your data secure.

You can run ParrotOS straight off the USB drive as well but that will somewhat limit your options but it's a pretty good way to get started quickly without compromising your existing OS.

https://parrotsec.org/

1.3 : Raspberry Pi

We had questions from a few users if they could use their Raspberry Pi's to help out. Yes, you can. Pi's are just mini computers that can do the same thing that laptops and desktops can do. Just keep in mind that they won't be as effective as a more powerful PC due to the diminished resources in a Pi. But everything helps and a Pi could run 24/7 on your network. Please visit this website if you want to know how to install Linux on your Pi:

https://www.techradar.com/how-to/how-to-install-ubuntu-on-the-raspberry-pi

Step 2: Conseal your Identity

Get yourself a good VPN service. A VPN hides your public IP address by substituting it for the public IP address of the VPN termination host or its internet breakout. So in case of an investigation your public IP will not show. Here's a list of VPN providers. Some of them are paid and others come with a free trial:

https://www.top10vpn.com/top10/free-trials/?v=header&bsid=c15ense1kw287&gclid=EAIaIQobChMIs8i9ouii9gIVnIODBx07PgGMEAAYAiAAEgJkkfD_BwE

If you know any other good (perhaps) free VPN services, please DM the group admin and he/she will make sure the information is dispatched in the next version of this document.

Please be aware that 99% of VPN services sell information to third parties. A few good free VPN providers are:

- TunnelBear : https://www.tunnelbear.com
- PureVPN : https://www.purevpn.com
- SurfShark : https://surfshark.com
- Proton VPN : https://protonvpn.com
- Express VPN (12$) : https://www.expressvpn.com
- airVPN : https://airvpn.org
- Cryptostorm : https://cryptostorm.is
- Perfect Privacy : https://perfect-privacy.com
- Mullvad VPN : https://mullvad.net

2.1 : Parrot OS and VPN:

If you're using ParrotOS, you may not need a VPN. (see STEP 2).

https://www.youtube.com/watch?v=6ICeYQvNmJ0&t=890s

If you use this, you do not need a VPN. Go to *Privacy* in the menu then *AnonSurf* and then start now. You're done, now you're using *the onion router*. And the advantage is that you can also use this as a Dos option.

2.2 : Install anon-surf on Kali :

https://cybernationalsecurity.net/how-to-install-anon-surf-on-kali-linux-step-by-step/

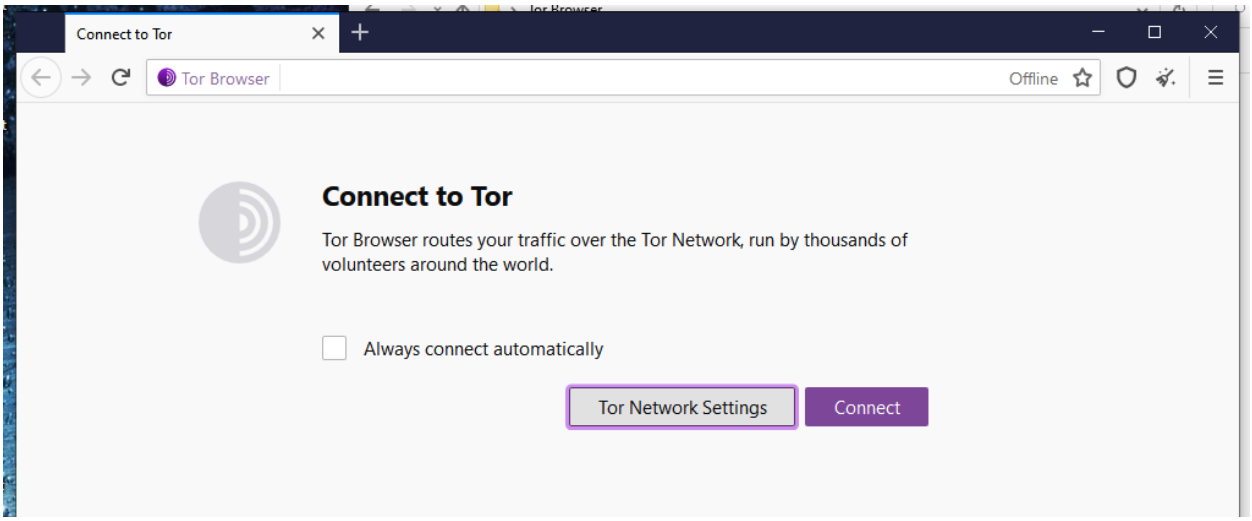
We received a good question from a member who had some concerns about the safety of VPN because the ISP you're connected to can see your public (real) IP. Yes, this is true. The ISP can indeed see your real IP address. But it doesn't matter. I will explain that to you in a minute. The ISP can see the following :

- That you use a VPN
- VPN server's address
- VPN protocol used
- Your real IP address
- Connection timestamps
- Amount of data transferred
- Encrypted data

Your ISP can see the VPN traffic itself. It is not difficult to tell that the IP address you are connecting to belongs to a VPN provider. The ISP, however, only sees the connections going to a VPN server and not the websites you visit. Your traffic is encrypted using a VPN protocol, such as IPsec or SSL. These protocols use strong encryption and a unique port they connect to. You can also tell which VPN protocol was used by the port number. It also knows the times when you establish a connection and how long you browse. If your ISP decides to inspect your contents – it can't. With a VPN it can see only the encrypted gibberish data stream. It is not possible to crack the encryption algorithms used by VPNs, therefore your traffic is secure.

Step 3 : Get TOR Browser

If you're thinking about using HTTP based (DDOS) attacks, get yourself the TOR browser. TOR stands for "The Onion Routing" which, as the name suggests, uses different layers and hops of routing in order to obscure the traceability of your terminal and let you remain anonymous.



TOR can be found here : https://www.torproject.org/

Opera Browser has a built-in VPN option :

https://blogs.opera.com/news/2016/09/how-to-set-up-a-vpn-mac-windows-linux/

NEVER EVER attack a target without proper concealment of your identity. You WILL go to jail otherwise.

3.1 iMAC Whonix

We got some questions from MAC users if they could participate as well. Of course you can !!! Install Whonix in a Virtual Box on your MAC and then harden it. Whonix utilizes TOR, which provides an open and distributed relay network to defend against network surveillance. However, you will need to configure it though. It does provide some security out of the box but you will need additional configuration to harden it. So after you've installed Whonix and fired it up , please visit :

https://www.whonix.org/wiki/System_Hardening_Checklist

Step 4 : Attack (Test) Programs

Get yourself a good attack (DDOS) program. On the sites themselves are examples on how to use them. If you have to bypass Cloudfare UAN anti-DDOS, you could use :

https://github.com/yottaiq/CloudAttack

Here are a few others (non Cloudfare) :

Slowloris

Slowloris is basically an HTTP Denial of Service attack that affects threaded servers. It works like this:

1. We start making lots of HTTP requests.
2. We send headers periodically (every ~15 seconds) to keep the connections open.
3. We never close the connection unless the server does so. If the server closes a connection, we create a new one keep doing the same thing.

This exhausts the servers thread pool and the server can't reply to other people. In order to run the attack, we need the logic of slowloris, however we won't write it by ourselves, instead, use the Python Slowloris implementation from an open source repository in Github.

https://github.com/gkbrk/slowloris

The script runs 150 sockets by default. After the installation just run :

$ python3 slowloris.py [*website url*] -s [*number of sockets*]

Bombardier

https://github.com/codesenberg/bombardier/releases/tag/v1.2.5

(example use : Example usage - ./bombardier-linux-amd64 --duration=240h --connections=1000 --latencies https://lenta.ru)

It maybe wise to run your query in a docker :

https://github.com/nitupkcuf/runner

[More information required]

DB1000N

Check our own program - Death by 1000 needles (DB1000N)

https://github.com/Arriven/db1000n

This is software for coordinated DDoS attacks on the occupier's infrastructure. The main advantage of this method is that users only need to run the program on a PC to carry out attacks, and all coordination will be carried out and configured by administrators with the support of cyber security specialists.

Instructions for use and all necessary links are on the main website:

https://hackmd.io/pl_ucHTWQUmO9ubmzRT1tQ

Please join everyone and download the program to your PC before the evening attacks, because then we will carry out the first attack with DB1000N. Stay tuned in the channel and look for upcoming updates.

GEEK INFO :

Here's a cool neat ARP Spoofing article, also known as ARP Poisoning actually used for Man in the Middle (MitM) attacks. This can be very effective if you happen to know the IP addresses of routers along the way.

https://medium.com/geekculture/simple-but-powerful-denial-of-service-dos-attack-8c7dfd60045f

4.1 HTML pages

D3pR4V3d (7ch4os4 Whoami) created a HTML page that you can copy and load in a TOR browser and you can target several sites at the same time. A little further up is explained how you can create a local copy from the online code. You don't need a VPN for this as long as you use your TOR browser. Follow the instructions on the Github page in order to create a local .html page that you can then run in your TOR browser. The author will make sure that if new targets arise, the script is updated. So bookmark this Github page ☺

https://github.com/D3pR4V3d/norussian

Coder1955Alpha created a javascript HTML, which you can copy-paste to a local html file and run it in your TOR browser. A little further up is explained how you can create a local copy from the online code. Please check out the Github page. If you are a graphical designer, please contact him/her so you can work together on a nice GUI for this script. The author will make sure that the targets are updates as soon as new targets come out so bookmark this page.

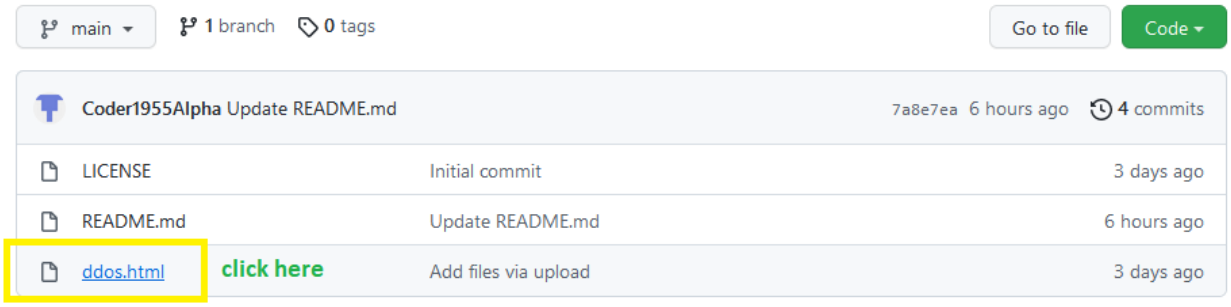
https://github.com/Coder1955Alpha/DDoS

If you don't feel comfortable with copying code and doing all kind of nerdy stuff because you're scared you're going to screw things up (or if you're going to bed) and still want to contribute and help us with the war effort, you can use any of the following website below, just leave it opened in your browser as long as possible:

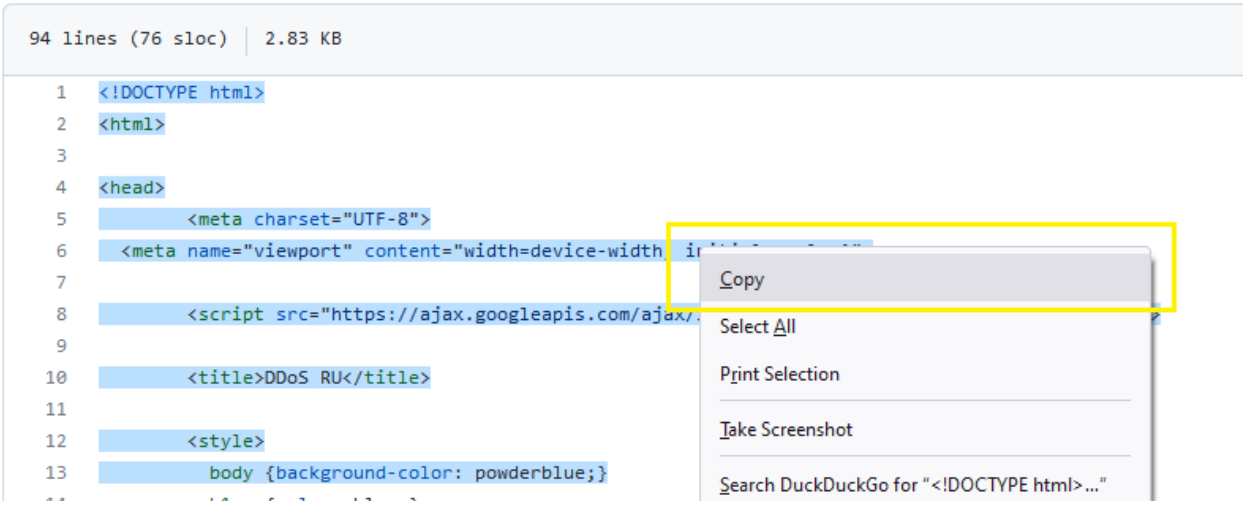
https://fuckyourussianwarship.netlify.app
https://ddosmonitor.pp.ua/

4.2 How to create a local HTML page (For Windows)

1. Open the github page and click on the file with the extension **.html**

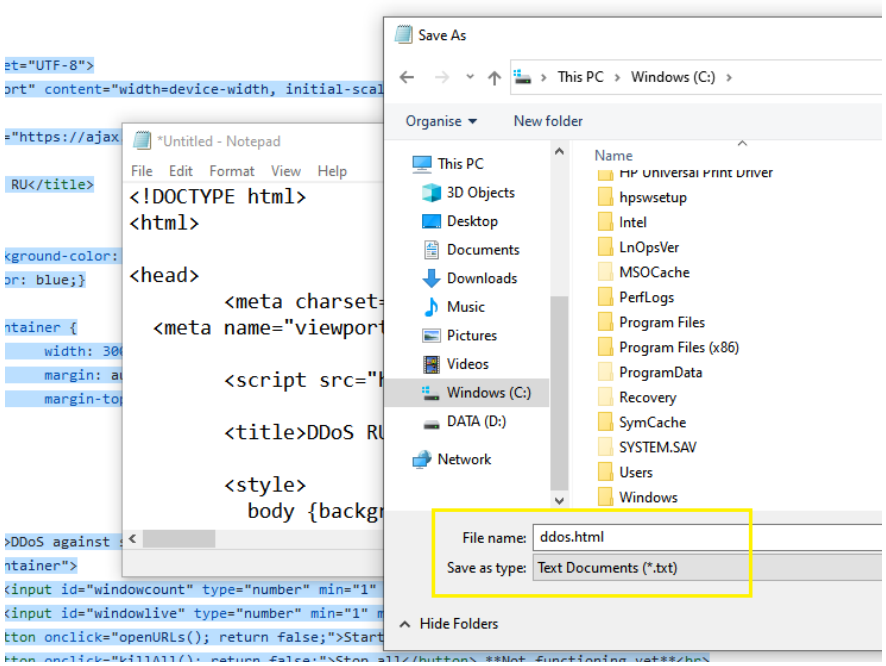


2. Select the code as you would normally select text in a document.



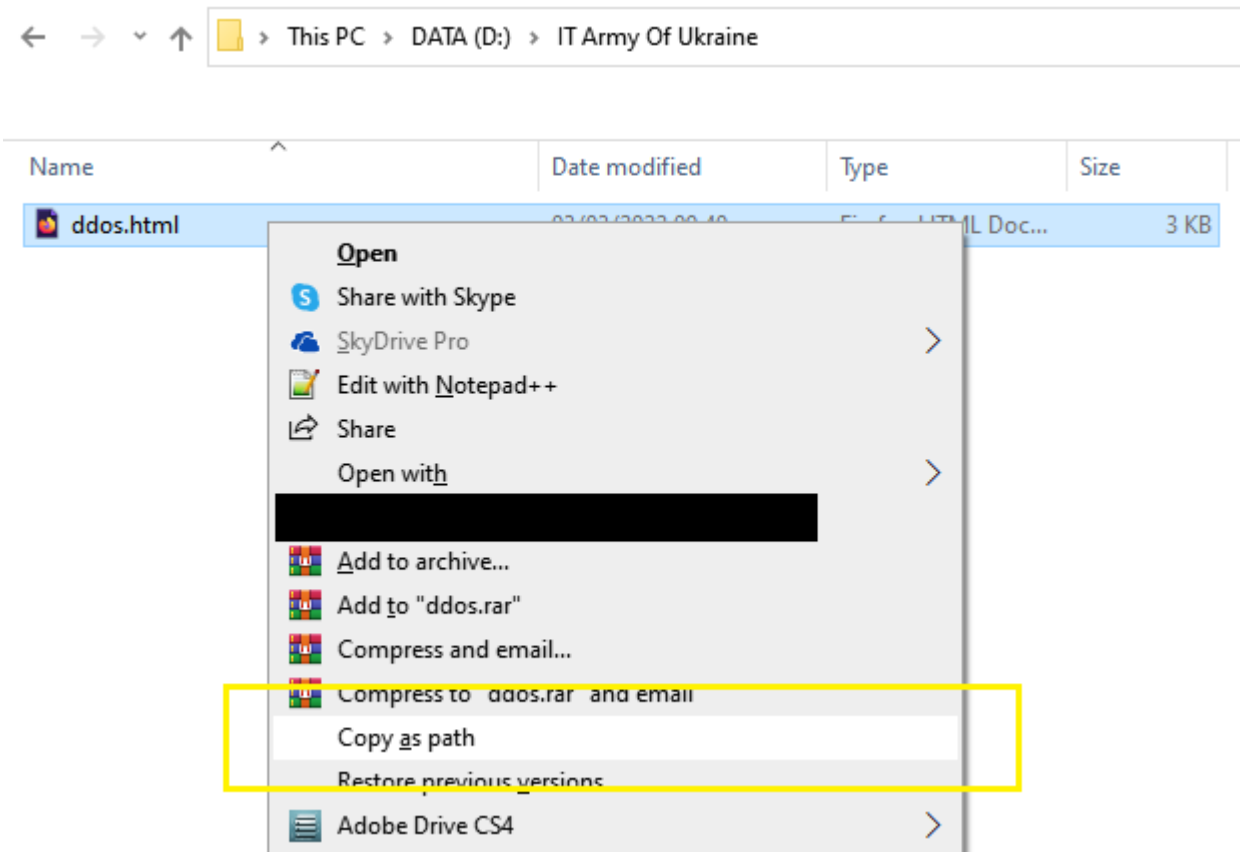
Don't use "Select All" because that will select the entire page and you only want the code.

3. Open a new notepad file and paste the copied code in the new file and save it somewhere locally on your computer. Make sure you change the extension of your new file is **.html**

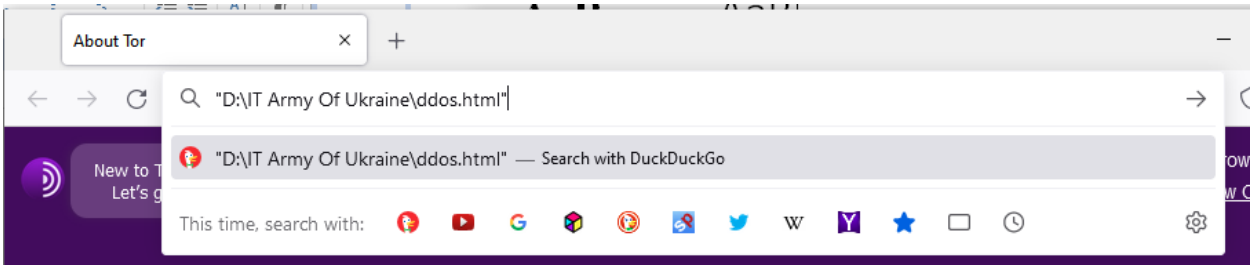


4. Find your file in 'Explorer', select the file by clicking ONCE (left mouse button), hold down the SHIFT key and right-click on the selected file. Select "Copy as path".

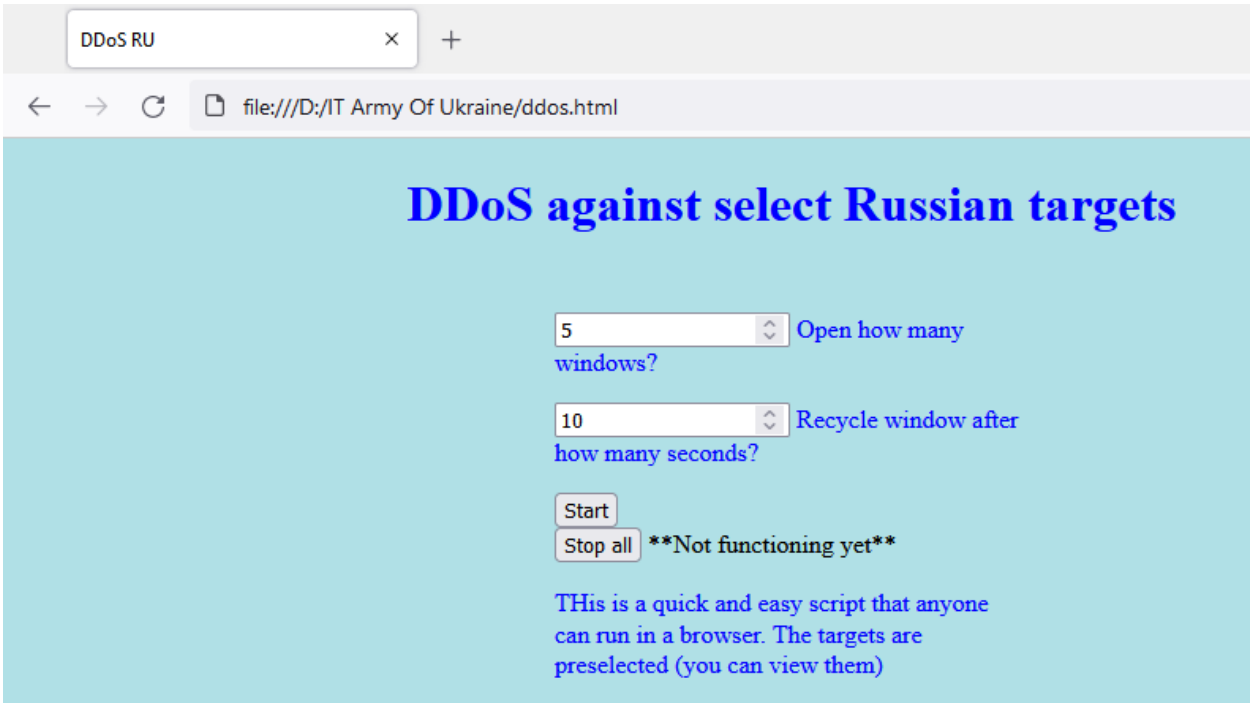
Be careful not to double click this file because it will open in your selected default HTML program, most likely a normal browser and you will be exposed.



5. Open your TOR browser and paste (CTRL-V) the copied path in the address bar of your TOR browser. You have to remove the double quotes ("") on each end or it won't open. Hit enter when you've removed the quotes.



6. Select your criteria based of your computers resources and available provider uplink (internet) bandwidth and off you go !!!



Step 5 (optional): SOCKS Proxy

If you're really paranoid you can also run your network connection through several proxy (socks) services but this is not strictly necessary. Here's a list of free proxy services (servers) :

https://spys.one/en/socks-proxy-list/

GEEK INFO :

SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. SOCKS5 optionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer). A SOCKS server accepts incoming client connection on TCP port 1080, as defined in RFC 1928.

Step 6 (optional): NMAP Port Scanner

If you want to scan ports of a remote host, you can install the tool *nmap* :

https://nmap.org/

Please read the manual carefully. NMAP is a very powerful tool with many options to discover open ports. A good site to learn quickly is :

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

For the WINDOWS users among us, there is a GUI for *nmap*, called *zenmap* :

https://nmap.org/zenmap/

It does the same thing except it comes with a nice user-friendly GUI (Graphical User interface).

GEEK INFO :

Anonymous also created a webpage with tools that you can use in order to help the war effort in Ukraine. Most tools will do the same as the tools described in this document, however they are for more advanced users. If you have no technical experience we suggest you follow the rules outlined in this document in order to stay safe and get yourself up and running in the shortest possible time.

Never the less, great work Anonymous !!

https://anonymousworldwide.com/2022/02/26/anonymous-tools-for-oprussia-ukraineunderattack/

TIPS and tricks :

TIP 1: NMAP

For anyone who has access to nmap already, nmap is pre-installed in Kali and ParrotOS.
Check if you have this script by running this in the terminal "locate http-slowloris.nse"
if you see this:

/usr/share/nmap/scripts/http-slowloris.nse

You can then use it on any desired IP.

nmap -vv --script http-slowloris --max-parallelism 400 <target IP>

TIP 2: DNS

We also recommend changing your DNS to 9.9.9.9. This is an open DNS recursive service for free security and high privacy since your local DNS service may not always give you what you need in terms of reliability.

https://www.windowscentral.com/how-change-your-pcs-dns-settings-windows-10

Another thing that will greatly improve your security is DNS over HTTPS.

TIP 3: Randomized MAC addresses

There's two controls for using random hardware addresses—one is for all Wi-Fi networks and the other is for the specific Wi-Fi network you choose. When you turn it on for all networks, random hardware addresses are used while your PC scans for networks and connects to any network. When it's turned on for a specific network you choose, random hardware addresses are used the next time you connect to that network.

https://support.microsoft.com/en-us/windows/how-to-use-random-hardware-addresses-in-windows-ac58de34-35fc-31ff-c650-823fc48eb1bc#:~:text=a%20specific%20network%3A-,Select%20the%20Start%20button%2C%20then%20select%20Settings%20%3E%20Network%20%26%20Internet,hardware%20addresses%20for%20this%20network

GEEK INFO :

Some of the information (webbrowsers) in this article was taken from the following article :

https://hackmd.io/pl_ucHTWQUmO9ubmzRT1tQ

Please check it out. It has a lot of additional information. Credit where credit due.

TIP 4: Spam sites like google maps and/or tripadvisor

Many people in Russia have no idea what's going on. It's a myth that every single Russian citizen supports the war. In fact, most Russian don't even know that Russia is the aggressor and that there even IS a war in the first place. So, in order to make them aware, you could go onto a popular website like tripadvisor or Trivago, find a Russian restaurant or hotel and give them a review.

Anonymous had a standard text that you could use, however in order to bypass spam filters you may alter the text slightly. Be creative with penetrating the minds of the average Russian citizen.

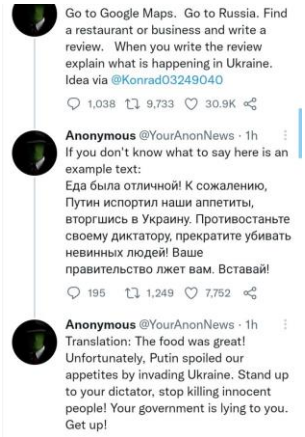
Here's the Russian text :

Еда была хорошей!
К сожалению, Путин испортил нам аппетит, подло развязав войну с Украиной.
Россияне, пора восстать против диктатора, пока еще не поздно! Во избежание смертей невинных людей и молодых российских солдат, которых кинули в мясорубку! Во имя мирного неба над вашими же головами, во имя будущего ваших же детей. Пожалуйста, встаньте, чтобы остановить эту бессмысленную войну. Украинцев убивают, ваши пацаны гибнут из-за сумасшедшего эго, имперских амбиций, непомерной жадности и кошелька!

You can change random Cyrillic letters such as "a, e, c, o" to Latin, they will look the same to get passed spam filters.

Translation :

The food was good!
Unfortunately, Putin spoiled our appetite by vilely unleashing a war with Ukraine.
Russians, it's time to rise up against the dictator before it's too late! In order to avoid the deaths of innocent people and young Russian soldiers who were thrown into a meat grinder! In the name of a peaceful sky above your own heads, in the name of the future of your own children. Please stand up to stop this senseless war. Ukrainians are being killed, your boys are dying because of a crazy ego, imperial ambitions, exorbitant greed and a wallet!



TIP 5: Find any Russian website you can and place a message.

Our valued member Insschnimp made a great tutorial on spamming Russian websites :

Russian websites where you can rate, blog or discuss as a quick way to get rid of messages. Sometimes they are checked before publishing, then at least the checker reads it. Maybe you can find websites where small posts are published directly. He managed to do that in a short time! He was able to post 5 messages extremely quickly.

If you want to read the full tutorial, search in the ITChatDiscussion Telegram Group of the IT Army of Ukraine for the file “how_you_can_help.pdf”. The file is clean. We checked so it’s safe to download.

Excellent work Insschnimp!

So please always remember this order :

- **Install OS**
- **Hide identity !!**
- **Attack (test)**