

ВАЖЛИВО!

- Перед тим, як починати будь-яку DDOS-атаку необхідно під'єднати VPN, який потрібно буде періодично змінювати (за винятку використання скриптів із проху)
- Старайтеся використовувати найефективніший спосіб атаки (див. Атака: найефективніший спосіб)
- Не атакуйте поодинокі цілі, дивіться в Телеграм-каналах, що атакують інші, та просто доєднуйтеся. Так у нас більше шансів “покласти ворожі сайти спатки”.
- Слава Україні!
- Русский военный корабль, иди нах*й!

Зміст (клікабельний)

Як під'єднати VPN?	2
Як перевірити, чи змінилася ваша IP-адреса.....	5
Атака: мегапростий рівень	6
Атака: простий рівень	9
Атака: середній рівень.....	13
Атака: продвинутий рівень.....	15
Атака: найефективніший спосіб	16
Перевірка результату DDOS-атак	17
Додаткові ресурси.....	18
Післямова	20

Як під'єднати VPN?

Найпростіше й найефективніше це користуватися готовими програмами, які можна скачати на свій комп'ютер і за допомогою однієї кнопки змінити своє розташування.

Якщо Ви знаєте інші способи зміни IP-адреси, або налаштування VPN, Ви можете використовувати їх, усе ап ту ю.

Нижче наведено перелік таких програм і посилання на них.

Просто скачуєте, встановлюєте, вибираєте будь-яку країну (у деяких випадках доцільно використовувати IP-адреси Росії, у деяких навпаки європейські, або американські IP, усе залежить від завдання).

Раджу скачувати по 2-3 програми. Бо буває, що одна із програм починає підлагувати.

Увага! Раджу використовувати Hotspot Shield, як основну програму для зміни вашої IP-адреси, зараз це найкращий вибір.

1. [Hotspot Shield](#)

Наразі для українців діє акція: Premium тариф протягом одного місяця. Просто реєструєтеся й скачуєте програму. Якщо ж акція вже не дійсна, то просто обираєте Premium тариф, оформляєте підписку на 1 місяць, підключаєте віртуальну картку (можна із 0 балансом) і користуєтеся Premium версією протягом 1 тижня. Потім не забудьте відключити картку, щоб не списало кошти за підписку.

+	-
Простий інтерфейс	
€ місяць Premium акаунту для українців	
€ російські IP	
Не лагає	

2. [F-Secure Freedom](#)

Тут реєструємося й далі скачуємо програму Freedom. Зараз вона доступна безкоштовно для українців протягом 30 днів.

+	-
Простий інтерфейс	Немає російських IP
Не потрібно прив'язувати свою картку	
Не лагає	

3. [Urban VPN](#)

Повністю безкоштовний. Варіант для тих, хто не хоче довго паритися із настройкою VPN.

+	-
Простий інтерфейс	Може лагати
Повністю безкоштовний	Російські IP у більшості випадків не працюють
Є російські IP	

4. [ClearVPN](#)

Зробили промо для українців (SAVEUKRAINE) із піврічним безкоштовним доступом. Через це його почали використовувати більшість українців і він почав дуже сильно підвисати. Тому зараз раджу використовувати інші програми.

+	-
Простий інтерфейс	Може дуже сильно лагати
Є промокод	Російські IP не працюють

5. [Windscribe](#)

Платний. І цим усе сказано. Можна знайти безкоштовні кращі альтернативи. Не рекомендую.

+	-
Простий інтерфейс	Платний
	Російські IP не працюють
	Може дуже сильно лагати

6. [KeepSolid VPN Unlimited](#)

Аналогічно до ClearVPN. Зробили промо для українців із підпискою на півроку, яке, на жаль, я зараз навіть не можу знайти (хто захоче використовувати цей VPN - науглите). Через це можливі сильні лаги. Зараз не рекомендую використовувати цю програму.

+	-
Простий інтерфейс	Немає російських IP
Є промокод	Може дуже сильно лагати

Як перевірити, чи змінилася ваша IP-адреса

Важливо! Після того, як Ви встановите й запустите VPN, необхідно перевірити, чи дійсно змінилася Ваша адреса (бувають випадки, що сервіс підлагує, або міняє адресу не на ту країну, що Ви обрали).

Ось посилання, де можна перевірити вашу теперішню локацію:

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

Атака: мегапростий рівень

Для тих, хто взагалі не хоче заморочуватися, є перелік сайтів і програм, які можна просто відкрити й вони самі будуть проводити атаки на певні сайти. Просто слідуйте інструкціям, які описані на самому сайті, або в програмі й вперед.

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати.

Як альтернатива VPN, можете скачати Tor Browser [за цим посиланням](#), після скачування в ньому ж відкрити вкладку із сайтами, які наведені нижче й насалоджуватися атаками на російські сайти 😊. При кожному новому входженні в браузер ваша IP буде мінятися. **Увага!** Для програм із пунктів 4 та 5 скачувати Tor Browser не доцільно.

1. [павутина.укр](#)

Атакує певний перелік російських сайтів, який можна змінювати.

Увага! Після відкриття цього сайту ваш ноутбук, або комп'ютер може виснути, будьте обережні.

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезаходити!

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

Атакує один із сайтів, який є актуальний на даний момент (сайт для атаки динамічно змінюється).

Сайт розроблений командою KiberBULL. [Посилання на їх Телеграм-канал.](#)

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезаходити!

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

Атакує стандартний перелік російських сайтів.

Ще один сайт, розроблений командою KiberBULL. [Посилання на їх Телеграм-канал](#).

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезаходити!

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

Атакує певний перелік сайтів, який самостійно динамічно змінюється, із використанням проксі. Вам потрібно лише встановити й запустити програму.

Програма розроблена командою UA Cyber SHIELD. [Посилання на їх Телеграм-канал](#). Переходите за посиланням, обираєте зручну для Вас мову, далі Найпростіший рівень, слідуєте інструкціям, встановлюєте програму й відкриваєте її в себе на комп'ютері.

Важливо! Не забувайте про увімкнений VPN! Tor Browser тут використовувати не доцільно!

5. [DB1000N](#)

Аналогічно до попередньої програми атакує певний перелік сайтів, який самостійно динамічно змінюється.

Програма розроблена командою DDOS по країні СЕПАРІВ (Кібер-Козаки). [Посилання на їх Телеграм-канал](#). Просто слідуєте інструкціям, встановлюєте програму й відкриваєте її в себе на комп'ютері.

Важливо! Не забувайте про увімкнений VPN! Tor Browser тут використовувати не доцільно!

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

І таке навіть створили! Гра, яку можна грати в браузері, а кожен твій крок проводить атаку на один із російських сайтів.

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезаходити!

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

Атакує стандартний перелік російських сайтів.

Увага! Після відкриття цього сайту ваш ноутбук, або комп'ютер може виснути, будьте обережні.

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезавантажити!

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

Атакує стандартний перелік російських сайтів.

Увага! Після відкриття цього сайту ваш ноутбук, або комп'ютер може виснути, будьте обережні.

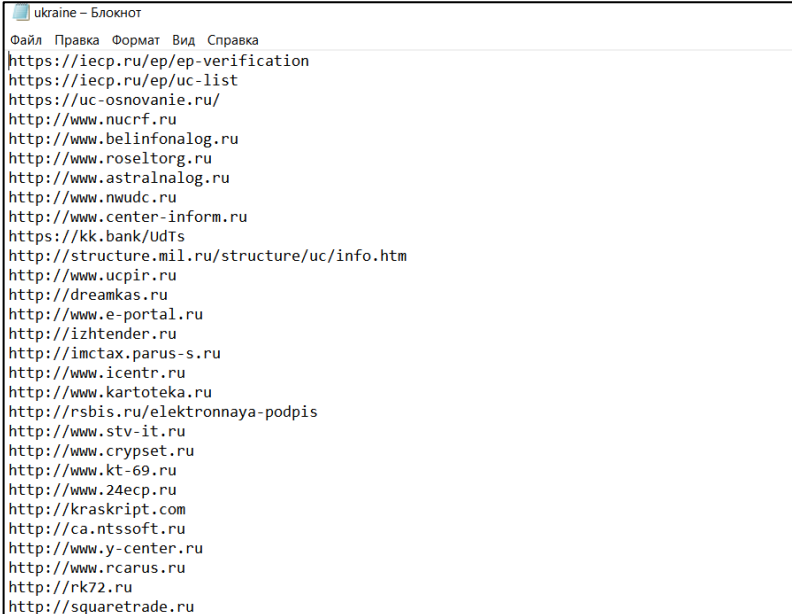
Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати, або Tor Browser, у який потрібно час від часу перезавантажити!

Атака: простий рівень

Для більшого маневру особистих дій того, хто атакує, можна використовувати вже готові програми, які доволі прості у своєму використанні.

1. Hello World

- Для скачування цієї програми користуємося [цією лінкою](#).
- Далі скачуємо архів і розпаковуємо його в однойменну папку.
- Заходимо всередину папки й у файл “ukraine.txt” просто передаємо сайти, на які хочемо здійснити атаку (кожен сайт із нового рядка, приклад на скріні нижче).



```
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.belinfonalog.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
```

- Якщо у Вас Windows, то просто запускаємо prau_ukraine_windows.exe, відкриється окреме вікно, як зображено на скріні нижче й насолоджуємося крахом РФ 😊.

```
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
```

- Якщо у Вас Linux або MacOS, то робимо наступне:
 - відкриваємо SystemPreference -> Security & Privacy -> Privacy -> Developer Tool -> Enable Terminal
 - відкривемо Terminal всередині папки, де знаходиться файл pray_ukraine_mac, або відкриваємо Terminal і просто переходимо в папку, де знаходиться файл pray_ukraine_mac
 - прописуємо команди:
 - `chmod +x pray_ukraine_mac`
 - `sudo ./pray_ukraine_mac`
 - насолоджуємося крахом РФ 😊

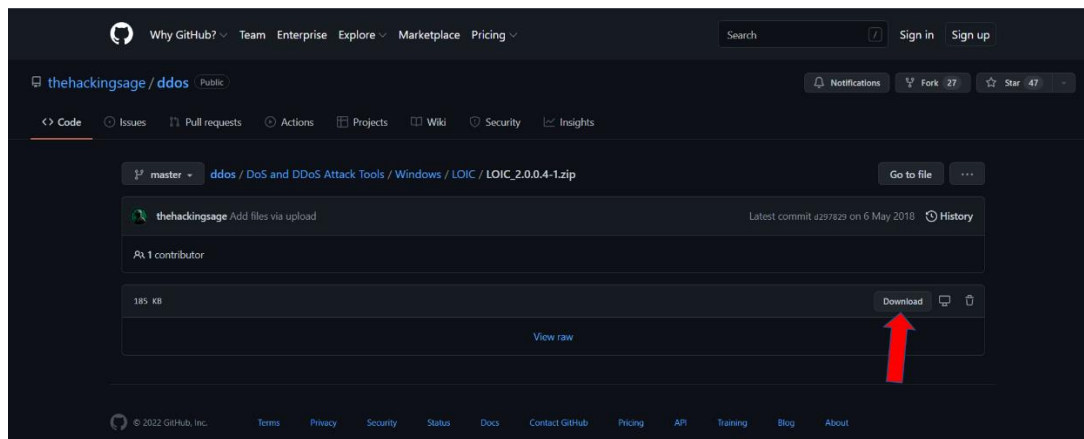
Програма розроблена Телеграм-каналом Поганці (Fire show). [Посилання на їх Телеграм-канал.](#)

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати.

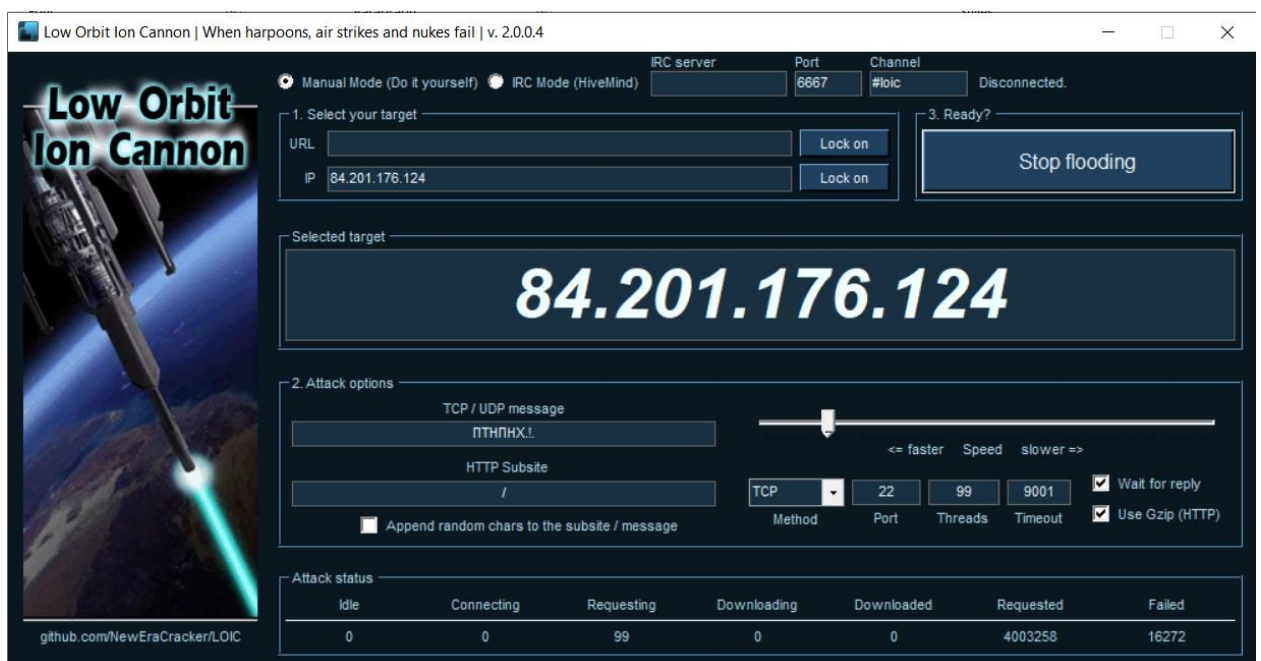
2. LOIC

Увага! Лише для користувачів Windows!

- Для скачування цієї програми користуємося [цією лінкою](#).



- Може бути так, що Ваш комп'ютер може блокувати скачування даного архіву, тому можете відключити антивірус (**на свій страх і ризик!**) на час скачування й встановлення даної програми. Проте після встановлення обов'язково увімкніть антивірус, він не мав би сваритися на дану програму.
- Розпаковуємо архів у будь-яку окрему папку.
- Всередині неї запускаємо файл LOIC.exe



- Далі або в поле URL передаємо фізичну адресу сайту, який ми хочемо атакувати (наприклад, <https://interfax.ru/>) і натискаємо Lock on, або в поле IP передаємо IP-адресу сайту й натискаємо Lock on (як зображено на екрані вище).

- У полі TCP/UDP message додаємо будь-який меседж, який Ви хочете донести до Росії 😊. Бажано його змінювати кожного разу, коли Ви міняєте свою IP-адресу.
- Ползунок Speed виставляємо або найлівіше, або трішки ближче до центру із лівого боку (як зображено на скріні вище).
- Далі вибираємо Method (TCP, HTTP або UDP). У більшості Телеграм-каналів, які публікують якісь цілі для атаки вже вказаний конкретний метод, тоді просто його обираємо.
- Далі обираємо порт у полі Port (поле біля поля Method, а не те, що вгорі, вгорі Port залишаємо дефолтним і рівним 6667). Порт це те, що вказується після двокрапки в IP адресі, наприклад, для 84.201.176.124:22 порт це число 22. У більшості Телеграм-каналів, які публікують якісь цілі для атаки вже вказаний конкретний порт, тоді просто його обираємо.
- **Важливо!** Якщо Method та Port не вказані, то пробуйте стандартні порти й методи для сайтів. Наприклад, TCP та 443, TCP та 22, HTTP та 80, можливі й інші варіанти.
- У полі Threads обираємо максимально можливе число, яке дозволяє вам комп'ютер, не видаючи помилку. Почніть із 200, далі 100 і тд. У моєму випадку це число 99.
- Усі решта поля залишаємо без змін.
- Натискаємо на кнопку IMMA CHARGIN MAH LAZER і насолоджуємося крахом РФ 😊.
- Як зрозуміти, що все працює? Якщо дуже збільшуються к-сть Requested та появляються Failed (скрін нижче), то Ви все робите правильно, так тримати.

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

Важливо! Не забувайте про увімкнений VPN, який потрібно час від часу змінювати.

Атака: середній рівень

Для тих, хто розуміє, як встановити й запускати Docker, є вже багато готових скриптів, які доволі легко запустити із локальної, або віртуальної машини.

[Ось посилання](#) на тьюторіал по тому, як встановити Docker на різні операційні системи і як запустити певний скрипт на Docker.

Усе прописано в *Інструкції DdoS*.

Також у *Використанні джерела та тьюторіали* є інші варіанти, як самостійно запускати скрипти із DDOS-атаками, використовуючи інші Докер контейнери, скрипти, написані на Python та інших мовах програмування.

Цей тьюторіал був складений командою DDOS по країні СЕПАРІВ (Кібер-Козаки). [Посилання на їх Телеграм-канал](#).

Також досить недавно появився Телеграм-канал Украинский Жнец, де в основному викладають гайди по Docker і Python скриптах. [Посилання на цей Телеграм канал](#). Усі необхідні статті Ви зможете знайти в закріплених повідомленнях каналу. Нижче наведено гайди, які доступні на даний момент:

- [Підготування віртуального робочого середовища для DDOS-атак](#)
- [DDoS Ripper Tutorial](#)
- [MHDDoS Tutorial](#)
- [Глибокий розбір MHDDoS](#)
- [Розвідка для DDOS-атак](#)
- [Атака "ізсередини" інфраструктури ворога \(proxychains\)](#)
- [Розбір MHDDoS proxy](#)
- [Обновлення proxy для MHDDoS proxy](#)

Важливо! Спершу потрібно розібрати [перший гайд](#), який дозволить розгорнути віртуальну машину. Далі обирайте скрипт на Ваш смак із наступних гайдів.

Увага! На даний момент практично всі команди, які публікують у себе в даному Телеграм-каналі Украинский Жнец ([посилання на цей Телеграм канал](#)) стосуються скрипту, описаного в [останньому гайді](#). Раджу розбиратися із ним.

Важливо! Перед тим, як запускати команди для атаки на якийсь ресурс можна перевіряти доступність цього ресурсу за допомогою команд:

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

Важливо! Якщо атакуєте із локальної машини, не забувайте про увімкнений VPN, який потрібно час від часу змінювати.

Атака: продвинутий рівень

За допомогою Докера, Docker контейнерів та інших скриптів на спеціальних сервісах можна розвертати безліч віртуальних машин, на яких паралельно можна запускати велику кількість DDOS-атак.

Нижче наведено tutoriали про те, як розвернути такі віртуальні машини на AWS, Digital Ocean, Azure та 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 \(video\)](#)

Атака: найефективніший спосіб

Команда DDOS Tutorial for all написала два дуже корисних гайди, які допоможуть Вам проводити атаки на ворожі сайти. Раджу усім, хто хоче ефективно й ефектно атакувати, розібратися із ними, налаштувати робочу машину й використовувати скрипт MHDDoS_proxu згідно із гайдом.

Якщо виникають будь-які питання, задавайте їх у коментарях під будь-якими постами в [цьому Телеграм-каналі](#).

- [Як розгортати віртуальні машини на Digital Ocean](#)
- [Детальний розбір MHDDoS_proxu](#)

Також у команди DDOS Tutorial for all з'явився ГітХаб репозиторій, де знаходяться вище наведені гайди й згодом будуть з'являтися нові.

- [Посилання на GitHub](#)

Перевірка результату DDOS-атак

Кожному із тих, хто атакує, хотілося б слідкувати за прогресом його атак, чи вони взагалі мають якийсь сенс і чи дають результат.

Нижче наведено два сервіси, де Ви можете передати або фізичну адресу сайту (наприклад, <https://interfax.ru/>), або IP-адрес із портом (наприклад, 84.201.176.124:22).

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

Також є сайт, де Ви можете за допомогою IP адреси знайти всю необхідну інформацію про цю IP адресу, як-от: відкритість портів (див Port Scanner), або чи сайт пінгується, чи ні (див Ping):

- <https://viewdns.info/>

Увага! Також нещодавно в Телеграм-каналі Український Жнец ([посилання на цей Телеграм канал](#)) вийшов гайд по тому, як правильно підготуватися до DDOS-атак. Усім раджу прочитати й розібратися, там є багато корисних посилань:

- [Розвідка для DDOS-атак](#)

Додаткові ресурси

Telegram-канали (пов'язані із DDOS):

- [DDOS по країні СЕПАРІВ \(Кібер-Козаки\)](#)
- [DDOS Tutorial for all](#)
- [ddos котики](#)
- [KiberBULL](#)
- [Украинский Жнец](#)
- [Zion](#)
- [UA Cyber SHIELD](#)

Telegram-канали (інші):

- [IT ARMY of Ukraine](#) (Кіберармія України)
- [Anti-Putin Hackathon](#) (Різні проєкти для перемоги над окупантом)
- [DataLeaks](#) (Витоки із різних російських баз даних)

Telegram-канали із постійною інформацією про те, як нагадувати світовому суспільству про напад Росії:

- [УкрТві Військо](#)
- [УкрІнста Військо](#)

Корисні GitHub репозиторії:

- [DDoS for all](#)
- [Оригінальний MHDDoS](#)
- [MHDDoS проху](#)
- [Украинский Жнец](#)
- [DB1000N](#)

[Ресурси для DDOS-атак](#)

Сайт із всією необхідною інформацією по Україні в часи війни:

<https://viyna.net/>

Корисний сайт, який дає змогу швидко конвертувати цілі, які дають в IT Army of Ukraine, у формат, який використовується для команд:

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

Слак-канал із різними проєктами для людей із сфери ІТ (для того, щоб пройти модерацію необхідно мати робочий LinkedIn акаунт):

[UA Tech Power](#)

Персональні дані російських користувачів:

[IT ARMY Leaks](#)

Післямова

- Із будь-якими питаннями звертайтеся в [цей Телеграм-канал](#) та пишіть їх у коментарях під постами.
- Слідкуйте за [GitHub репозиторієм](#), будемо добавляти туди нові гайди.
- Буду дуже вдячним як за поширення посилання на Телеграм-канал DDOS Tutorial for all (https://t.me/+Z_LFYsLfmmM4YmUy), так і за поширення цього файлу із ТutorialsPoint.

Увага!

- Ви самі обираєте, чи виконувати атаки на російські сайти, чи ні!
- Автор даної інструкції не несе відповідальності за використання цієї інструкції!
- Слава Україні!
- Русский военный корабль, иди нах*й!