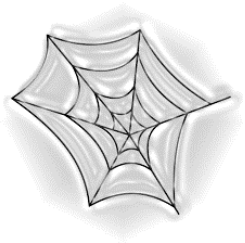


ბნელი ქსელი

თეორია და პრაქტიკა

სტატია განკუთვნილია სტუდენტებისთვის და, ასევე ყველასთვის, ვისაც ბნელი ქსელი (Dark Web) აინტერესებს

პაატა გოგიშვილი

ინფორმატიკის დოქტორი, ილიას სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

paatagog@gmail.com, paata.gogishvili@iliauni.edu.ge

www.max.ge

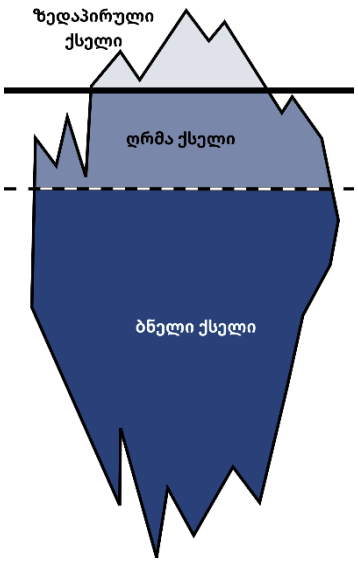
განმარტება

ინტერნეტი აისბერგს ჰგავს. რასაც ჩვენ ყოველდღიურად ვიყენებთ, მხოლოდ აისბერგის მწვერვალია, მას „ზედაპირულ ქსელს“ უწოდებენ. ზედაპირის ქვეშ არის უზარმაზარი „ღრმა ქსელი“, სადაც ონლაინ აქტივობების უმეტესობა ხდება საჯარო დახარისხების გარეშე. უფრო ღრმად, ჩვენ ვხვდებით „ბნელ ქსელს“, სამეფოს, რომელიც მოცულია საიდუმლოებით, ინტრიგებითა და საშიშროებით.

გახსოვდეთ, რომ ბნელი ქსელი არ არის ცალსახად ცუდი, ისევე როგორც ზედაპირული ქსელი არ არის ყოველთვის კარგი. როგორც ნებისმიერი ხელსაწყო, მისი გამოყენების ეთიკურობაც გამოყენების მეთოდებსა და მიზნებზეა დამოკიდებული. პატივი ეცით სხვების პირადულობას და საიდუმლოებას, მოერიდეთ მავნე შინაარსს და ყოველთვის დაიცავით ეთიკური ნორმები.

ზედაპირული ქსელი

ზედაპირული ქსელი არის ის ინტერნეტი (უფრო სწორად ინტერნეტის ის ნაწილი), რომელსაც ყოველ დღე ვიყენებთ. იგი შედგება ვებსაიტებისგან, რომლებიც დახარისხებულია საძიებო სისტემების მიერ, (მაგალითად Google ან Bing). ამ საიტებზე სტანდარტული ვებ ბრაუზერების გამოყენებით შევდივართ და მათი შინაარსი საჯაროდ არის ხელმისაწვდომი. საიტებზე არის ახალი ამბები, ონლაინ მომსახურებები, სოციალური მედია, სასარგებლო ინფორმაცია და მრავალი სხვა რამ.



ღრმა ქსელი

ზედაპირული ქსელის ქვემოთ არის ღრმა ქსელი. იგი მოიცავს მონაცემთა ბაზებს, კერძო ქსელებს და შიგთავსს, რომლებიც საძიებო სისტემებისთვის მიუწვდომელია. თქვენი ელექტრონული ფოსტა, ონლაინ ბანკინგი და აკადემიური მონაცემთა ბაზები ღრმა ქსელის ნაწილია. ეს რესურსები საჭიროებს შესვლის პაროლებს ან სპეციალურ ნებართვებს წვდომისთვის.

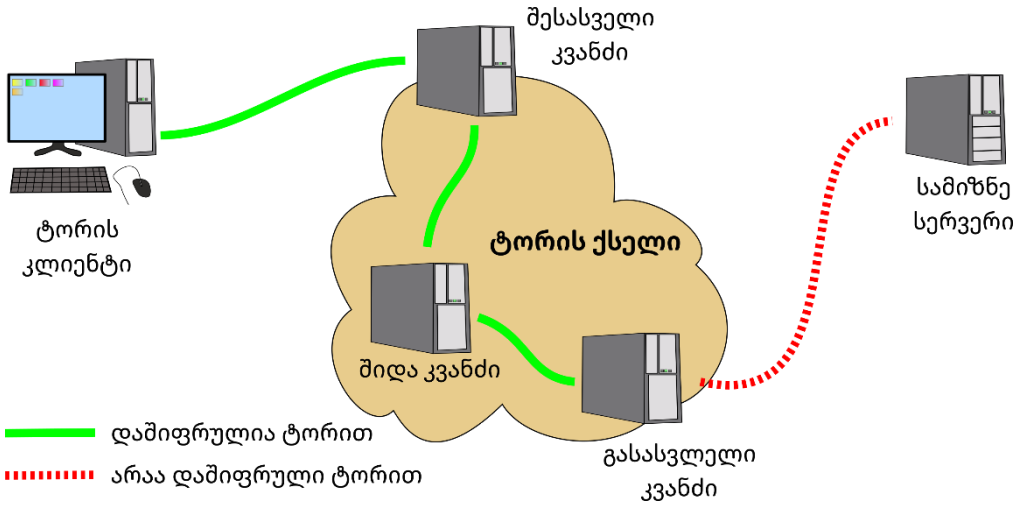
ბნელი ქსელი

ბნელი ქსელი განზრახ დამალულია და მასზე წვდომა შესაძლებელია მხოლოდ სპეციალიზებული პროგრამის Tor-ის (The Onion Router) გამოყენებით. ეს არის ადგილი, სადაც პირადულობა არის დაცული. ვებსაიტებს აქვთ დომენის გაფართოება "`.onion`". გარდა იმისა, რომ ეს არის სივრცე, სადაც პირადულობის შენარჩუნება შესაძლებელია, მას ბნელი მხარეც აქვს - იგი მასპინძლობს უკანონო საქონლის ბაზრებს, კრიმინალური მოქმედების ფორუმებს და ინტერნეტის

სხვა ფარულ კუთხეებს. Tor-ის ბროუზერი შემდეგი მისამართიდან უნდა გადმოწეროთ: www.torproject.org

ბნელი ქსელის მოწყობის მექანიზმი

ბნელი ქსელის ბირთვი არის Tor (The Onion Router) ქსელი. Tor არის უფასო, ღია კოდის პროგრამა, რომელიც საიდუმლო კავშირის საშუალებას იძლევა ინტერნეტით. ეს მიიღწევა მონაცემების მარშრუტიზაციის გზით მოხალისეების მიერ მართული სერვერების, ან კვანძების ქსელის მეშვეობით.



როდესაც მომხმარებელს სურს ბნელ ვებ-გვერდზე წვდომა მათი მონაცემები იშიფრება და იგზავნება Tor კვანძების ჯაჭვის მეშვეობით. ჯაჭვს მრავალი კვანძი აქვს და მათი სიმრავლე ხახვის ფენებს მიამსგავსეს, აქედან მოდის ამ ქსელის სახელწოდებაც. ჯაჭვის თითოეული კვანძი აკლებს თავდაპირველი შიფრის მხოლოდ თითო ფენას, რაც უკიდურესად ართულებს ინფორმაციის თავდაპირველი წყაროს მიკვლევას. ქსელის კვანძები შეიძლება დაიყოს სამ კატეგორიად: შესვლის კვანძები, შიდა კვანძები და გასასვლელი კვანძები. ამჟამად რამდენიმე ათასი კვანძია ჩართული ტორის ქსელში. რეალურ დროში ტორის ქსელის მასშტაბების შესახებ ინფორმაციის მისაღებად შემდეგი მისამართით შეგიძლიათ ისარგებლოთ https://metrics.torproject.org/networksize.html

შესასვლელი კვანძი

მონაცემების გადაცემა იწყება შესასვლელი კვანძიდან (ასევე უწოდებენ მცველ კვანძს). ეს არის პირველი კვანძი ჯაჭვში. მან იცის თქვენი IP მისამართი, მაგრამ არ იცის რას აკეთებთ ინტერნეტში, რადგან თქვენი მონაცემები დაშიფრულია. შესვლის კვანძი გადასცემს თქვენს მონაცემებს ჯაჭვის შემდეგ კვანძს.

შიდა კვანძი

შემდეგი, თქვენი მონაცემები იგზავნება ერთი ან რამდენიმე შიდა კვანძის მეშვეობით. ამ კვანძებმა იციან მხოლოდ ჯაჭვის წინა და შემდეგი კვანძების IP მისამართი. მათ არ აქვთ ცოდნა თავდაპირველი წყაროს ან საბოლოო დანიშნულების შესახებ. თითოეული შიდა კვანძი გაშიფრავს დაშიფრული ინფორმაციის ერთ ფენას და გადასცემს მონაცემებს შემდეგ კვანძს. მონაცემთა გადაცემას, როგორც წესი, რამდენიმე შიდა კვანძი უძღვება. სურათზე სიმარტივისთვის მხოლოდ ერთი შიდა კვანძია ნაჩვენები.

გასასვლელი კვანძი

საბოლოოდ, მონაცემები აღწევს გასასვლელ კვანძს. გასასვლელი კვანძი გაშიფრავს დაშიფვრის ბოლო ფენას და აგზავნის თქვენს მოთხოვნას დანიშნულების ვებსაიტზე ან სერვისზე ბნელ ქსელში.

მნიშვნელოვანია, რომ გასასვლელი კვანძის IP მისამართი (და არა თქვენი) ჩანს ვებსაიტზე ან სერვისზე, რომელსაც თქვენ მიმართავთ. ეს უზრუნველყოფს პირადულობას, რაც გადამწყვეტია ბნელი ქსელის მომხმარებლებისთვის.

ბნელ ქსელში არსებული ვებსაიტები ხშირად იყენებენ დომენის სპეციალურ გაფართოებას სახელწოდებით "`.onion`". ამ ვებსაიტებზე წვდომა შესაძლებელია მხოლოდ Tor ქსელის საშუალებით. ისინი შექმნილია პირადულობის უზრუნველსაყოფად როგორც საიტის მასპინძლის, ასევე მისი სტუმრებისთვის. როდესაც თქვენ შედიხართ `.onion` საიტზე, თქვენი მოთხოვნა იგზავნება Tor ქსელის საშუალებით ისე, როგორც ზემოთ იყო ახსნილი.

დაშიფვრის და მარშრუტიზაციის მრავალი ფენის კომბინაცია კვანძების ქსელში უზრუნველყოფს პირადულობისა და დაცულობის მაღალ ხარისხს Tor ქსელის მომხმარებლებისთვის. ეს ტექნოლოგია უკიდურესად ართულებს სხვა მომხმარებელთა მიერ, მათ შორის სამთავრობო უწყებებს და კიბერკრიმინალებს მიერ, მონაცემთა წარმოშობის მიკვლევას ან მომხმარებლის გამოვლენას.

თუმცა, მნიშვნელოვანია აღინიშნოს, რომ მიუხედავად იმისა, რომ Tor უზრუნველყოფს პირადულბის კარგ დაცვას, იგი ვერ უზრუნველყოფს აბსოლუტურ უსაფრთხოებას. მომხმარებლებმა მაინც უნდა დაიცვან კიბერუსაფრთხოების ჰიგიენა და ფრთხილად იყვნენ პირადი ინფორმაციის გაზიარების დროს, ასევე არ უნდა ჩაერთონ ბნელი ქსელის უკანონო ქმედებებში.

ბნელი ქსელის რამდენიმე საიტი

DuckDuckGo

DuckDuckGo არის პირადულობაზე მოგეზილი ძებნის სისტემა. გაითვალისწინეთ, რომ საძიებო სისტემა განკუთვნილია ზედაპირული ქსელის ვებ-საიტებს საპოვნელად, იგი არ ეძებს Tor საიტებს.

https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

Ahmia

Ahima არის ძებნის სისტემა `.onion` საიტებისთვის.

http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

The Hidden Wiki

The Hidden Wiki (დამალული wiki) არის ბნელი ვებსაიტი, რომელიც წარმოადგენს სხვადასხვა ვებსაიტებსა და რესურსების ბმულების საცავს. მასში შედის ბლოგების, ინფორმაციის საცავების, ტექნიკური სახელმძღვანელოების და სხვა რესურსების ბმულები. ეს არის ამოსავალი წერტილი მომხმარებლებისთვის, რომლებიც ეცნობია ბნელ ქსელში არსებულ მრავალფეროვან ინფორმაციას.

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion

Dark Net Forum

Dark Net Forum არის ბნელი ქსელის ფორუმი, სადაც მომხმარებლებს შეუძლიათ საიდუმლოდ განიხილონ სასურველი თემები. იგი ზედაპირული ქსელის ფორუმებს მსგავსია, თუმცა იცავს პირადულობას. მომხმარებლები შესაძლოა ჩაერთონ ტექნოლოგიებთან, კიბერუსაფრთხოებასთან, პირადულობის ინსტრუმენტებთან და პოლიტიკურ აქტივობასთან დაკავშირებულ დისკუსიებში.

http://3otgxq7d33rwspxfquwkqlp7r4yoicofniypk7hcxxqefrwhptqp7zad.onion

Market Place

Market Place არის ბნელი ქსელის ბაზრობა. მიუხედავად იმისა, რომ იქ ივაჭრება კანონიერი პროდუქტები, როგორიცაა ციფრული ხელოვნება და პროგრამული უზრუნველყოფა, იგი აგრეთვე

შეიცავს უკანონო პროდუქციასაც, როგორიცაა ნარკოტიკები და ჰაკერული მომსახურება. ტრანზაქციები ხდება კრიპტოვალუტების გამოყენებით - როგორც წესი, Bitcoin-ის საშუალებით.

http://shoprypxphsufyldigdn34kbjbsnjnrmv2z34yc5al5lkmveqcbex2qd.onion

გაითვალისწინეთ, რომ იმ მომენტისთვის, როცა თქვენ ამ სტატიას კითხულობთ, მისამართები შეიძლება უკვე შეცვლილი იყოს. თუ ღრმა ქსელში უკვე სცადეთ საიტების მოძიება, დარწმუნდებოდით, რომ ეს არც ისე სასიამოვნოა, როგორც ზედაპირულ ქსელშია. მიუხედავად ამისა, ღრმა ქსელს აქვს თავისი უპირატესობები, რის შესახებაც ჩვენ უკვე გვაქვს გარკვეული ინფორმაცია.

კრიპტოვალუტების როლი ბნელი ქსელის ფულად ტრანზაქციებში

ბნელმა ქსელმა სახელი გაითქვა სხვადასხვა უკანონო ქმედებით, მათ შორის არალეგალური საქონლისა და მომსახურების ყიდვა-გაყიდვით. კრიპტოვალუტები, განსაკუთრებით ბიტკოინი, მნიშვნელოვან როლს ასრულებს ამ საიდუმლო ციფრულ სფეროში ფულადი ტრანზაქციების განხორციელებაში.

კრიპტოვალუტები გვთავაზობენ ფსევდოპირადულობის ისეთ დონეს, რომელსაც ტრადიციული ფინანსური სისტემები ვერ აღწევენ. ბიტკოინის ტრანზაქციები აღირიცხება საჯარო ჟურნალში, რომელსაც ეწოდება ბლოკჩეინი, თუმცა იგი ამჟღავნებს მონაწილე მხარეების ვინაობას. ამის ნაცვლად, ტრანზაქციები ასოცირდება ასონიშნიან მისამართებთან, რაც უზრუნველყოფს პირადულობის მაღალ ხარისხს. ბნელი ქსელის მომხმარებლები ამ ფუნქციას იყენებენ ტრანზაქციების განხორციელებისას თავიანთი ვინაობის დასამალად.

კრიპტოვალუტის მომხმარებლები ცდილობენ გაექცნენ ტრადიციულ ფინანსურ ინსტიტუტებს და უსაფრთხოდ და საიდუმლოდ განახორციელონ საერთაშორისო ფულადი გზავნილები.

აღსანიშნავია, რომ Tor და blockchain ორივე დეცენტრალიზებული სისტემაა მსგავსი მიზნებით: პირადულობის უზრუნველყოფა და მომხმარებლის თავისუფლების ხარისხის ამაღლება.

Tor ქსელი ბლოკჩეინის ტექნოლოგიის გამოგონებამდე შეიქმნა. იგი შეიმუშავეს როჯერ დინგლედინმა, ნიკ მეთიუსონმა და პოლ სივერსონმა 1990-იანი წლების ბოლოს. ქსელი პირველად ამუშავდა და საჯაროდ ხელმისაწვდომი გახდა 2002 წელს.

ბლოკჩეინის ტექნოლოგია, რომელიც ეფუძნება კრიპტოვალუტებს, როგორიცაა ბიტკოინი, გამოიგონა პიროვნებამ ან ჯგუფმა ფსევდონიმით Satoshi Nakamoto. პირველი სტატია სახელწოდებით "Bitcoin: A Peer-to-Peer Electronic Cash System", გამოქვეყნდა 2008 წლის ოქტომბერში. თავად ბიტკოინის ქსელი ამოქმედდა 2009 წლის იანვარში.

`.onion` ვებ საიტის შექმნა და Tor-ის ქსელში განთავსება

საიტის შექმნა და მისი განთავსება Tor-ის ქსელში საკმაოდ მარტივია.

პირველ რიგში უნდა დააყენოთ პროგრამა Tor:

```
sudo apt install tor
```

შემდეგ უნდა დააყენოთ ვებ სერვერი, მაგალითად Apache:

```
sudo apt-get install apache2
```

თქვენი სასურველი ვებ გვერდის HTML შიგთავსი ჩაწერეთ `/var/www/html/index.html` ფაილში, ანდა, თუ ჯერ არაფერი გაქვთ მოფიქრებული, შემდეგი ფრაგმენტი გადაიტანეთ პირდაპირ:

```
<!DOCTYPE html>
<html>
<head>
```

```
    <title>Hello Tor</title>
</head>
<body>
    <h1>Hello, Tor World, მოგესალმებით ტორიდან!</h1>
</body>
</html>
```

დაარედაქტირეთ Tor-ის კონფიგურაციის ფაილი `/etc/tor/torrc`. ჩაწერეთ (ან მოხსენით კომენტარები) შემდეგი სტრიქონები:

```
HiddenServiceDir /var/lib/tor/mywebsite/
HiddenServicePort 80 127.0.0.1:80
```

ეს ბრძანებები ტორს ატყობინებს, რომ შექმნას საიდუმლო მომსახურების დირექტორია `/var/lib/tor/mywebsite/` და მე-80 პორტზე შემომავალი მოთხოვნები აქ გადმოამისამართოს.

გადატვირთეთ Tor-ის სერვისი კონფიგურაციის შეცვლილი ფაილის ასამოქმედებლად შემდეგი ბრძანებით:

```
sudo systemctl restart tor
```

გაიგეთ თქვენი `.onion` მისამართი ფარული სერვისის დირექტორიიდან:

```
sudo cat /var/lib/tor/mywebsite/hostname
```

ეს ბრძანება მოგცემთ თქვენი საიტის `.onion` მისამართს, რომელიც წარმოადგენს "`.onion`"-ით დაბოლოებულ სიმბოლოების შემთხვევით სტრიქონს.

თქვენი საიტი მზადაა და განთავსებულია Tor-ის ქსელში.

გახსენით Tor ბრაუზერი კომპიუტერში და შეიყვანეთ თქვენი .onion მისამართი მისამართების ზოლში.

საჭიროების შემთხვევაში შეგიძლიათ წაშალოთ ეს საიტი.

პირველ რიგში წაშალეთ თავად ვებ საიტის შემცველი ფაილი შემდეგი ბრძანების გამოყენებით:

```
sudo rm /var/www/html/index.html
```

შემდეგ წაშალეთ Tor-ის საიდუმლო მომსახურების დირექტორია, რომელიც იყო დაკავშირებული თქვენს ვებ საიტთან:

```
sudo rm -r /var/lib/tor/mywebsite/
```

ამ ბრძანებაში, ცხადია, რომ "`mywebsite`" უნდა შეცვალოთ იმ დირექტორიის სახელით, რომელიც Tor-ის კონფიგურაციის ფაილში მიუთითეთ

გააჩერეთ და აკრძალეთ Tor-ის მომსახურება:

```
sudo systemctl stop tor
sudo systemctl disable tor
```

პირველი ბრძანება აჩერებს მომსახურებს. მეორე ბრძანება Tor-ის მომსახურების ჩართვის თავიდან არიდებისთვის არის, როცა სისტემა თავიდან ჩაიტვირთება. Tor-ის სერვისის ხელახლა გასააქტიურებლად `sudo systemctl enable tor` ბრძანება შეგიძლიათ გამოიყენოთ.

გააჩერეთ და აკრძალეთ Apache-ის ვებ სერვერი:

```
sudo systemctl stop apache2
sudo systemctl disable apache2
```

პირველი ბრძანება აჩერებს მომსახურებას. მეორე ბრძანება Apache-ს ვებ სერვერის ჩართვის თავიდან არიდებისთვის გამოიყენება, როცა სისტემა თავიდან ჩაიტვირთება. Apache-ს ვებ სერვერის ხელახლა გასააქტიურებლად `sudo systemctl enable apache2` ბრძანება შეგიძლიათ გამოიყენოთ.