FANTAZYA'DA YASAKLARI SAVMAK: TOR NETWORK'ÜNDE WEB SİTESİ NASIL AÇILIR?

ZİYAHAN ALBENİZ - ZİYAHAN@ARKAKAPİDERGİ.COM

Arka Kapı Dergi 9. Sayısında yayımlanan, Fantazya'da Yasakları Savmak: TOR Network'ünde Web Sitesi Nasıl Açılır? adlı makaleyi sizlerle paylaşıyoruz.

Bu makale *"Yazının, bilgi ve düşüncenin özgürce üretilip, paylaşılabilmesi çabalarına mütevazi bir katkı olarak değerlendirilmesi"* arzusu ile Ziyahan Albeniz tarafından kaleme alınmıştır.

—

İnsanlık bugüne dek pek çok devrimi yaşadı. Ateşi bulduk, hayvanları evcilleştirip toprağı işledik. Bilimsel ve sanayi devrimleri, yeşil devrim olarak bilinen topraktaki verimliliğin artması, hepsi birer devrimdi. Ama 90'ların sonunda kitleler ile buluşan İnternet ise bütün bu devrimlerin taçlandığı apayrı bir süreç oldu.

Bilginin üretilmesi ve paylaşılması inanılmaz derecede kolaylaştı. Bir web sitesi açıp dünyanın öbür ucundaki insanlarla bilgilerinizi ve fikirlerinizi paylaşmak son derece kolaydı. Devletler ve teknoloji devletleri kol kola girerek fikirlerin özgürce filizlendiği bu ortamı iğfal etmeye (kandırmaya) çalışıyorlar. Yer yer de başarılı olduklarını söyleyebiliriz.

Fantazya isimli distopik ülkede ise durum daha karanlık. Artık onların izni olmadan bir web sitesi açmak neredeyse imkansız. Hem açsanız bile kısa bir süre sonra bir tebligat ile kapatılması, sunuculara ve verilere el konulması işten bile değil.

Adım adım hem bir servis sağlayıcı olarak siz; hem de ziyaretçileriniz izlenebilir. Fantazya'da ve dünyanın diğer baskıcı rejimlerinde ziyaret ettiğiniz web sitesi nedeniyle çeşitli suçlara maruz kalabilirsiniz. "Demokrasi beşiği", üzerinde güneş batmayan Britanya'da bile konuşulan böylesi yasalar, birbirlerini yasak ve zorbalıkta taklit etmekte mahir diğer yönetimlere de ilham verecektir şüphesiz.

Peki Fantazya'nın yurttaşları daha da genel olarak dünyanın özgür düşünen, bilim ve düşünce üreten insanları bir otoriteden icazet almadan, onların hışmından korkmadan bir web sitesi açamayacaklar mı artık? Tabii ki hayır! Onların insafına mahkum değiliz. Dünyanın her yerinde hacker kültürüne sadakatle bağlı "meraklılar" yepyeni yöntemlerle baskıcı otoritelere nanik yapmayı sürdürüyor.

Bunlardan biri de gönüllülerin destekleri ile yaşamını devam ettiren TOR Network'ü ve onun üzerinde çalışan Onion Servisleri. Bu servisler size tüm otorite ve onlara boyun eğen servis sağlayıcılarından, domain sağlayıcılarından bağımsız web sitesi açma imkânı sunuyor.

Bu yazımızda TOR Network'ünde bir web sitesi nasıl kurulur açıklamaya çalışacağız.

TOR Network'ünde bir sitem olsun, dünya bana vız gelir!

TOR network'ü özet olarak kullanıcının IP'sini gizlemek için internet paketlerini gönüllü bilgisayarlar (relay) üzerinden aktaran bir protokol. Protokolün çalışmasına dair ayrıntılar bu yazının konusu değil. Fakat Arka Kapı Dergi 2. Sayıda Muhammet Enes Özen tarafından kaleme alınan TOR yazısı bu hususu tüm tafsilatları ile açıklıyor. www.arkakapidergi.com'da da ücretsiz olarak yayımlandığı için okurlar rahatlıkla burada kendisi için açık olmayan ayrıntılar ile ilgili o yazıya müracaat edebilirler.

TOR, 2003 yılında TOR Button adıyla bir tarayıcı eklentisi olarak başladığı yaşamına, gördüğü hüsnü kabul neticesinde ayrı bir browser olarak devam etme kararı aldı.

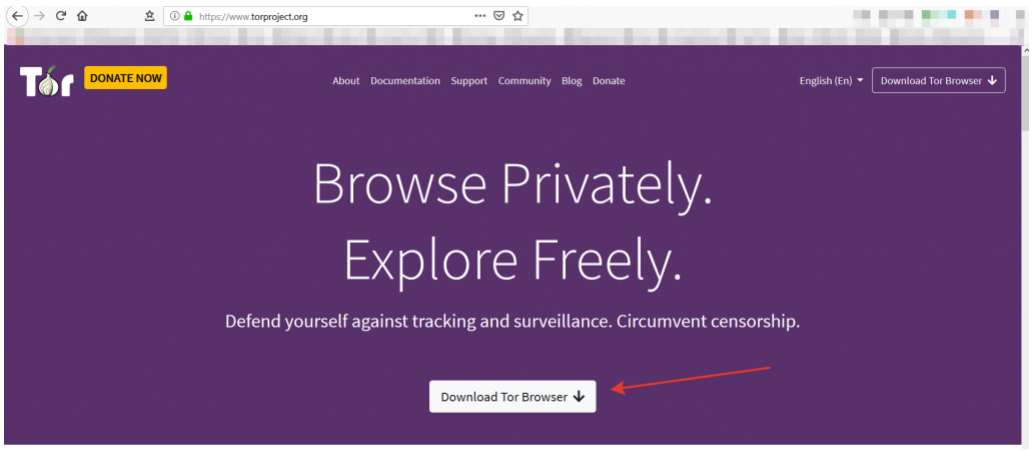
2004 yılından sonra ise sadece kullanıcıların IP'lerini gizlemek değil, aynı zamanda da TOR Services bugün ise ONION Services adı verilen bambaşka bir hizmeti de harikalar yelpazesine ekledi: Web sitesi sahiplerine, TOR networkünde kendi web sitelerini servis etme imkânı! Bu sayede ne domain sağlayıcılarına ne de hosting sağlayıcılarına mahkum olmadan TOR networkünde, gizliliğinizi de muhafaza ederek web sitesi servis edebileceksiniz.

Bu yazı, okur kitlesinin ortalaması baz alınarak Windows işletim sistemi üzerinde hazırlandı. Talimatların çoğunu *Nix işletim sistemlerinde de uygulayabilirsiniz.

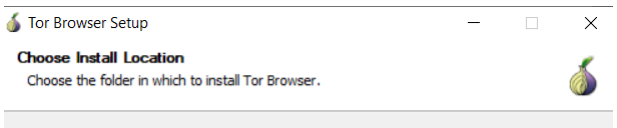
ONION Servislerinin Ayrıntıları

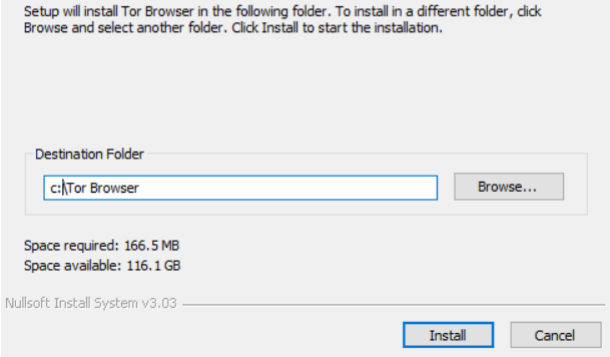
Yazının devamında TOR Network'ü üzerinden sunulan web sayfaları için ONION Servisleri tabirini kullanacağız. Yani TOR Network'ünde bir web sitesi sahibi olmak aslında bilgisayarınızda bir ONION Servisi başlatmak manasına geliyor.

TOR Browser Bundle'ı bilgisayarınıza www.torproject.org adresinden kurabilirsiniz. Mozilla Firefox tabanlı TOR Browser ve beraberinde TOR servisi sisteminize yüklenecek.



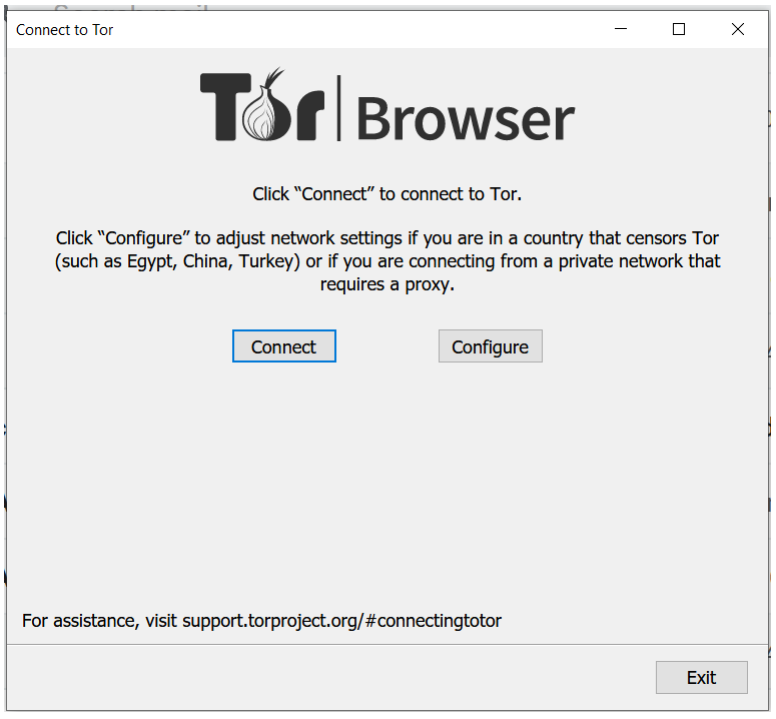
Tor Browser kurulum dosyasını indirdikten sonra, ilgili dosyayı tıklayarak kurulumu başlatabilirsiniz.





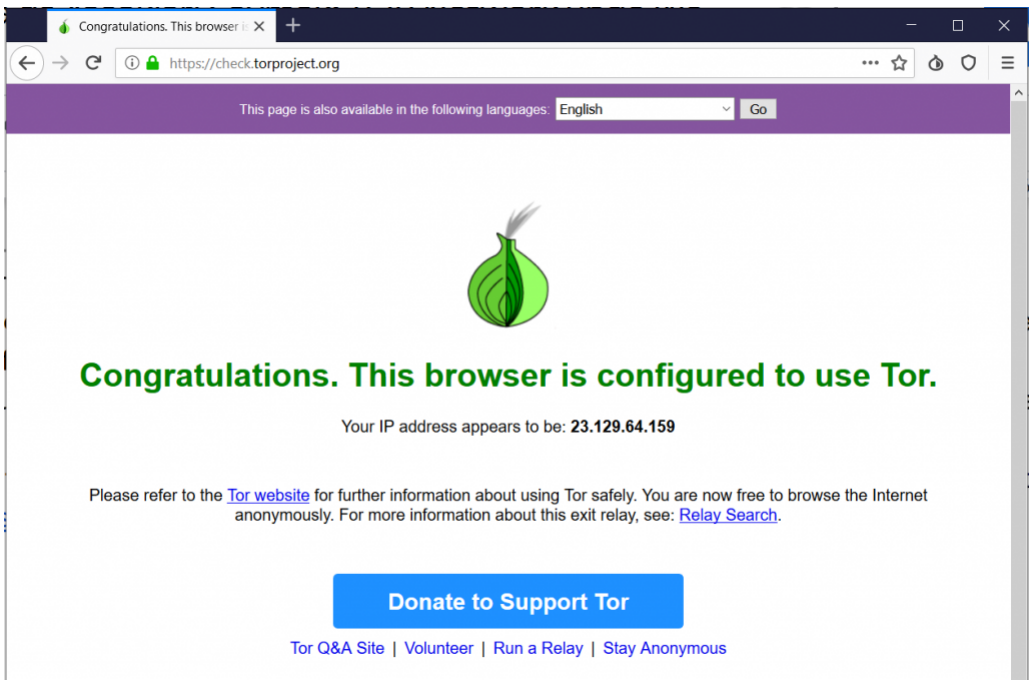
Bendeniz Tor Browser'ın kurulacağı dosya yolu olarak c:\Tor Browser dizinini seçtim. Yazıda da sonraki ayarlar için bu klasöre referans verilecektir.

Kurulum bittikten sonra TOR Browser'ı açtığınızda TOR Network'üne bağlanmanız için bir ekran belirecek.



Bu ekranda TOR Network'üne doğrudan bağlanmayı seçebileceğiniz gibi, Fantazya vb. ülkelerde yaşıyorsanız muhtemelen TOR Network'üne erişim otoriteler tarafından engellendiği için Configure seçeneğine tıklayarak bir Bridge üzerinden TOR Network'üne bağlanma opsiyonunu kullanabilirsiniz. Ayrıntılar yazının başlangıcında referans verdiğim yazıda mevcut.

Her şey tamamsa, TOR Network'üne bilgisayarımızın sağlıklı bir şekilde bağlandığını test etmek için https://check.torproject.org sitesini ziyaret edebiliriz:



Evet! Asayiş berkemal. Şimdi işin geri kalan kısmına geçebiliriz.

TOR Browser'da Küçük Bir Nüans

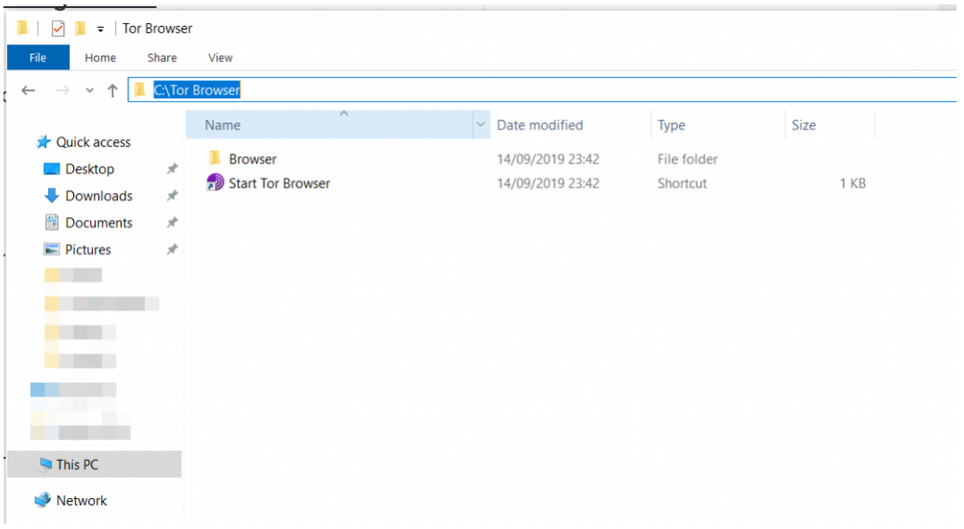
Dikkatli okur şunu fark edecektir. **Yalnızca TOR Browser üzerinden erişimler TOR Network'ü üzerinden hedefe aktarılıyor. Diğer tarayıcılar üzerindeki web trafiğiniz olması gerektiği gibi hedefe varıyor ve IP adresiniz ifşa oluyor.**

Diğer bir mesele de TOR Network'ü üzerinde bir web sitesi yayımlayacaksak hizmetin kesintisiz bir biçimde devam etmesi gerekiyor. Peki bu durumda TOR Browser hep açık mı kalmalı?

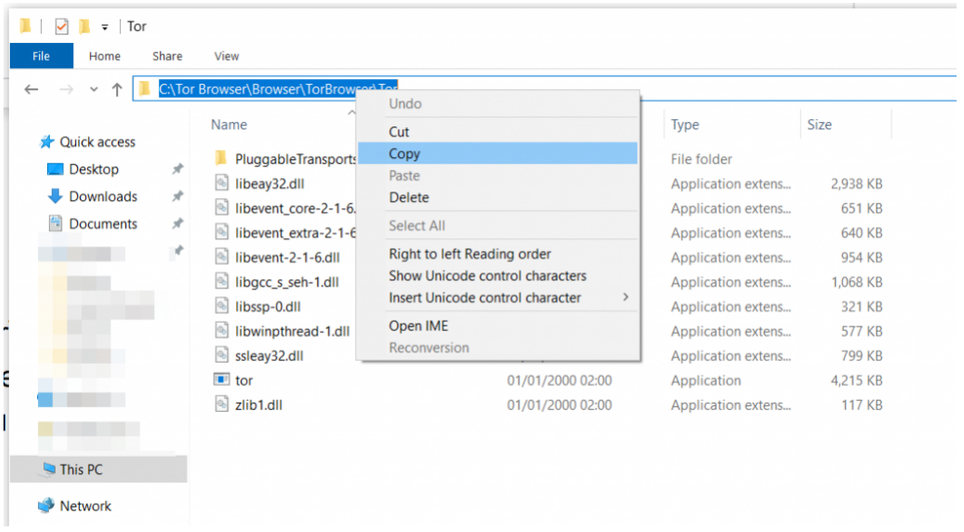
Tabii ki hayır! Şimdi birkaç küçük ayarla TOR Browser ile birlikte tarayıcımıza kurulan fakat sadece tarayıcı ile birlikte başlatılan TOR servisini bir Windows servisine dönüştüreceğiz.

Hazır mıyız?

Hatırlarsanız TOR Browser'ın c:\Tor Browser dizinine kopyalanmasını belirtmiştik. Şimdi bu dizine gidelim:



Bu dizin içerisinde bulunan Browser\Tor Browser\Tor dizinine girelim ve dizin yolunu kopyalayalım:

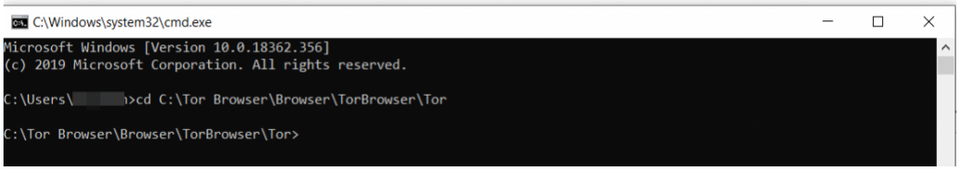


Şimdi Windows Komut İstemi'ni açacak ve mevcut dizini bu dizin olarak değiştireceğiz:

Başlat > *Çalıştır*'a yahut *Start* > *Run*'a **cmd** yazarak enter tuşuna basınız. Karşınıza siyah bir ekranda Windows Komut İstemi çıkacak:

```
cd C:\Tor Browser\Browser\TorBrowser\Tor
```

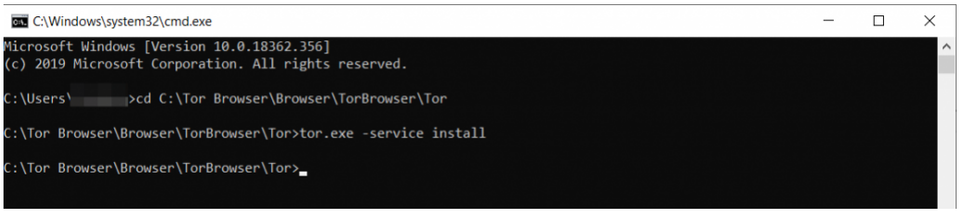
Yazarak dizin içerisine girelim:



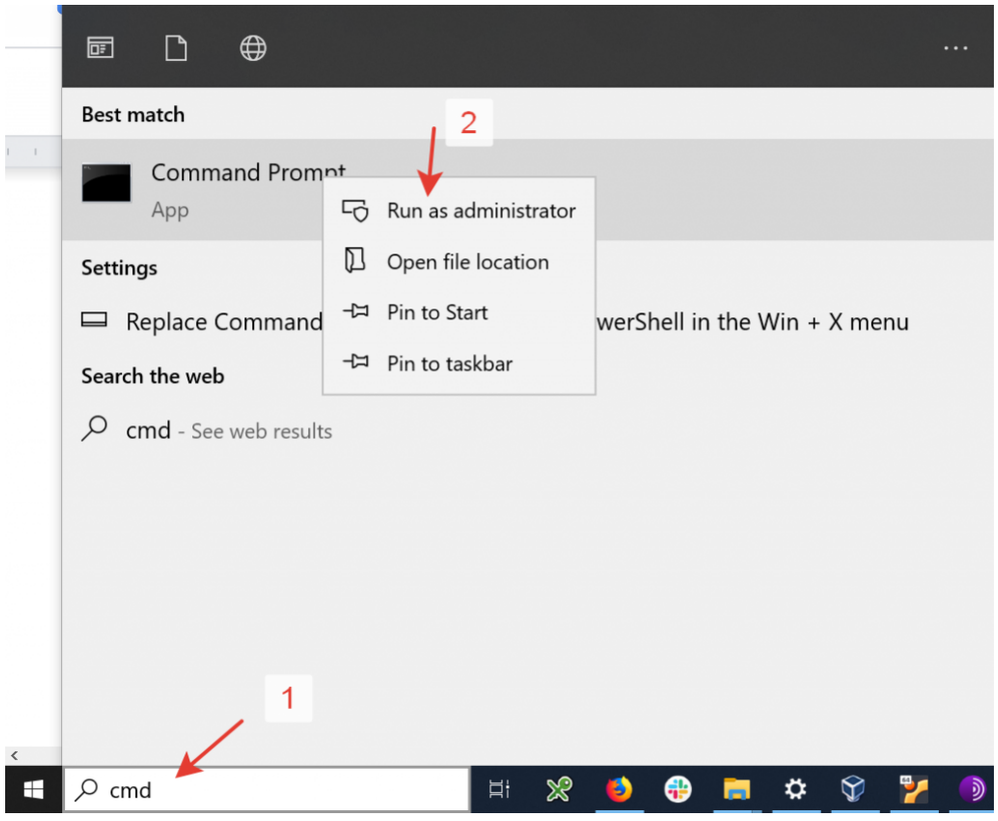
Şimdi *tor.exe* isimli programın bir Windows servisi olarak her işletim sistemi açılışında başlatılması talimatını vereceğiz. Böylelikle Tor Browser açık olsun ya da olmasın herhangi bir programın internet trafiğini Tor Network'ü üzerinden gönderebileceksiniz.

İlgili komutumuz:

```
tor.exe -service install
```

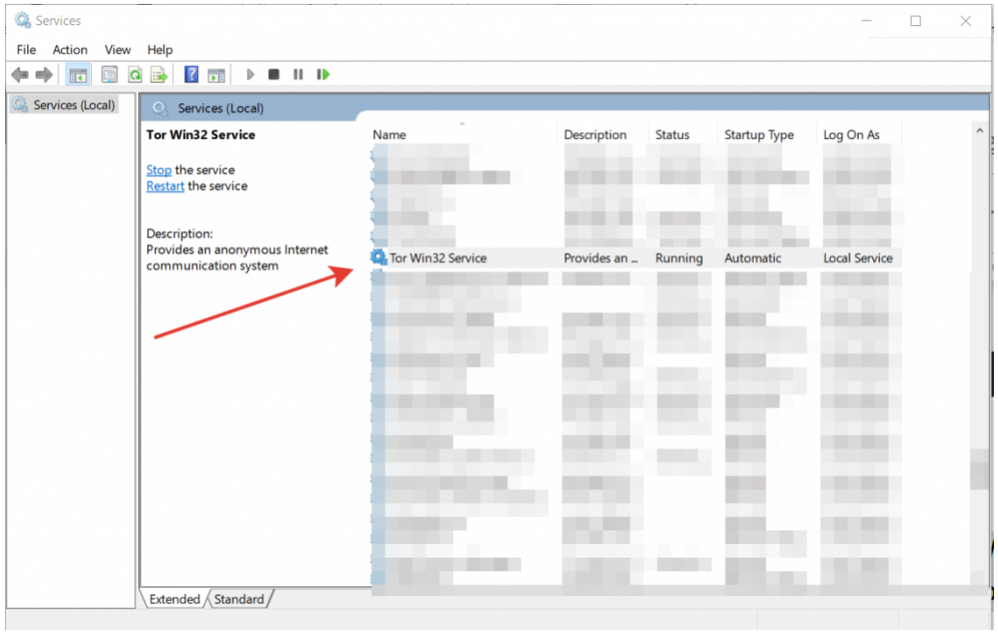


Küçük bir hatırlatma, eğer Windows işletim sistemi üzerinde hali hazırda kullandığınız hesabın yönetici yetkileri yoksa komut çalışmayacaktır. Windows Komut İstemi'ni yönetici yetkileri ile açtıktan sonra aynı işlemi tekrarlayabilirsiniz:



tor.exe isimli uygulama artık bir Windows servisi olarak kullanılmaya hazır. Windows servislerine bir göz atarak sonucu doğrulayabiliriz:

Başlat > Çalıştır yahut Start > Run ekranına **services.msc** yazarak Windows'daki tüm servislerin listesine ulaşabilir ve listede Tor Win32 Service isimli girdiyi kontrol edebilirsiniz:



Artık herhangi bir tarayıcının proxy (vekil sunucu) ayarlarından SOCKS5 tipinde 127.0.0.1 **port 9050'yi girerek TOR Browser'ı açmak zorunda kalmadan TOR Network'ü üzerinden web sitelerini gezebilirsiniz. Bu işlemden sonra https://check.torproject.org'u ziyaret ederek trafiğin TOR network'ü üzerinden aktığını doğrulamanızı öneririm.**

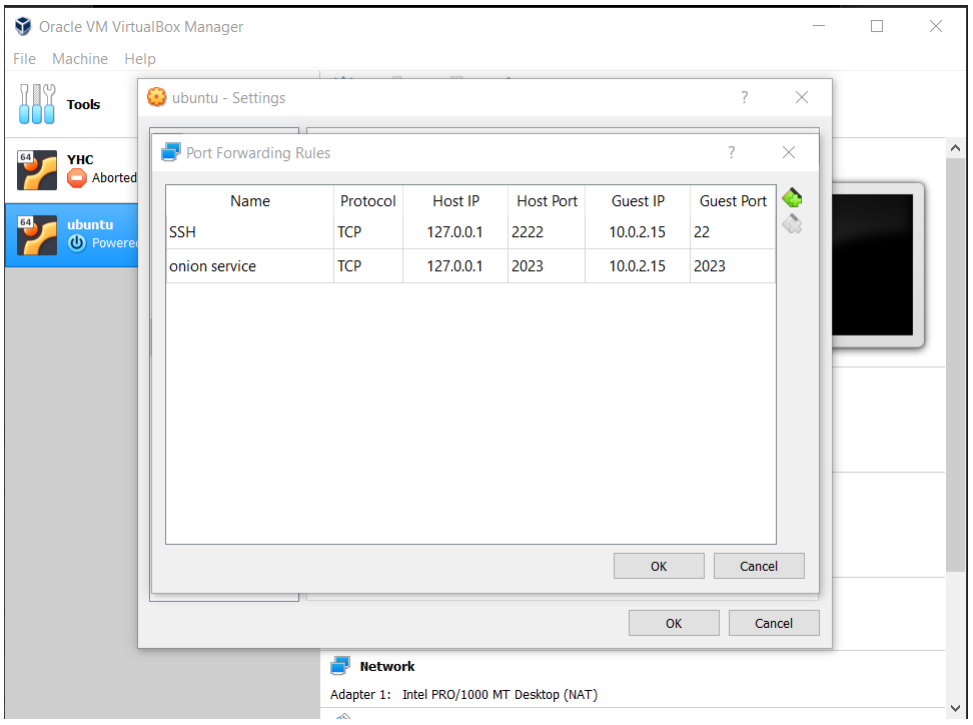
İlk aşamayı tamamladık. Şimdi ONION Servislerine biraz daha ayrıntılı bakabiliriz:

Sunucumuzu Hazırlayalım

Bir web sitemiz olacak, dedik. Fantazya'da hosting servislerini kullanırsak, bir tebligatlık ömrü olduğuna da değindik. Öyle ise iş başa düştü. Web sitemizi kendimiz host edeceğiz.

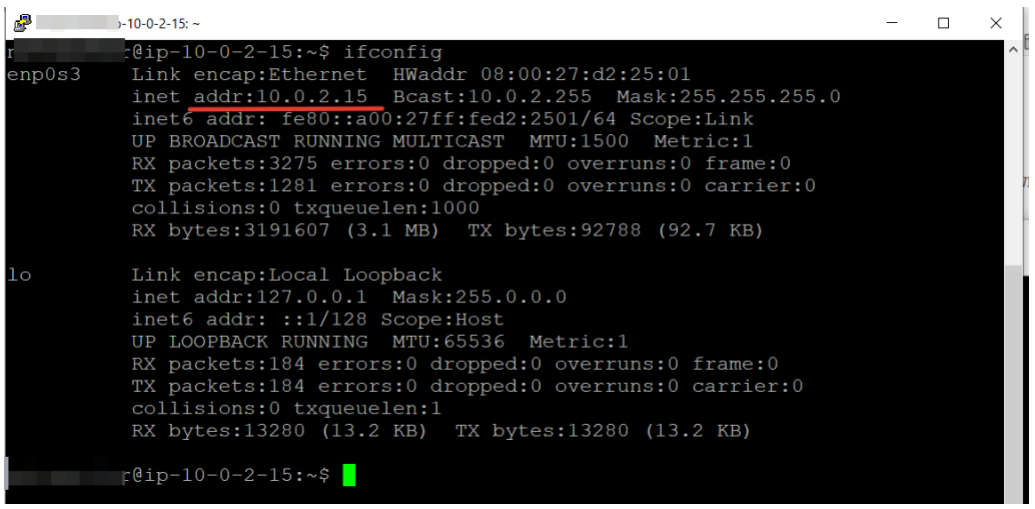
Bununla ilgili olarak ben VirtualBox sanallaştırma yazılımı üzerindeki bir makineyi kullanacağım.

Ubuntu işletim sistemi kurulu bu makinenin ayarlarını NAT arkasında konumlanacak şekilde ayarladım. Yani bu sanal makineye sadece host makine (benim makinem) üzerinden ulaşılabilecek. Dışarıdan herhangi bir isteğe kapalı olacak.



Web Server yani sunucu yazılımı olarak tercihimi Nginx'ten yana kullandım (www.nginx.com) Nitekim TOR'un web sitesinde de ONION servis işletecekler için önerilen sunucu yazılımlarından biri Nginx.

Aşağıdaki ekran görüntüsünden de anlaşılacağı üzere sunucum NAT arkasında 10.0.2.15 IP adresini kullanıyor:

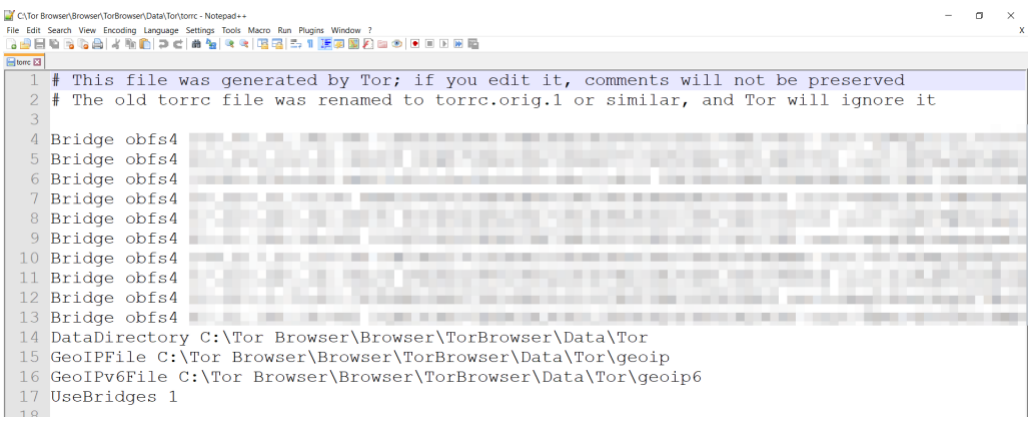


Şimdi ONION Servis ayarlarımıza geçelim.

torrc Sen Bizim Her Şeyimizsin!

torrc TOR'un kullandığı bir konfigürasyon dosyası. Bir ONION servisi başlatmak istediğimizi de bu konfigürasyon dosyası vasıtası ile söyleyeceğiz.

torrc dosyasına ulaşmak için C:\Tor Browser\Browser\TorBrowser\Data\Tor yolunu kullanabilir, herhangi bir metin editörü ile bu dosyayı görüntüleyebilirsiniz:



TOR'da bir ONION servisi kullanmak istediğimizi söylemenin yolu, bu dosyaya aşağıdaki iki satırı eklemek:

```
HiddenServiceDir C:\my_onion_service
```

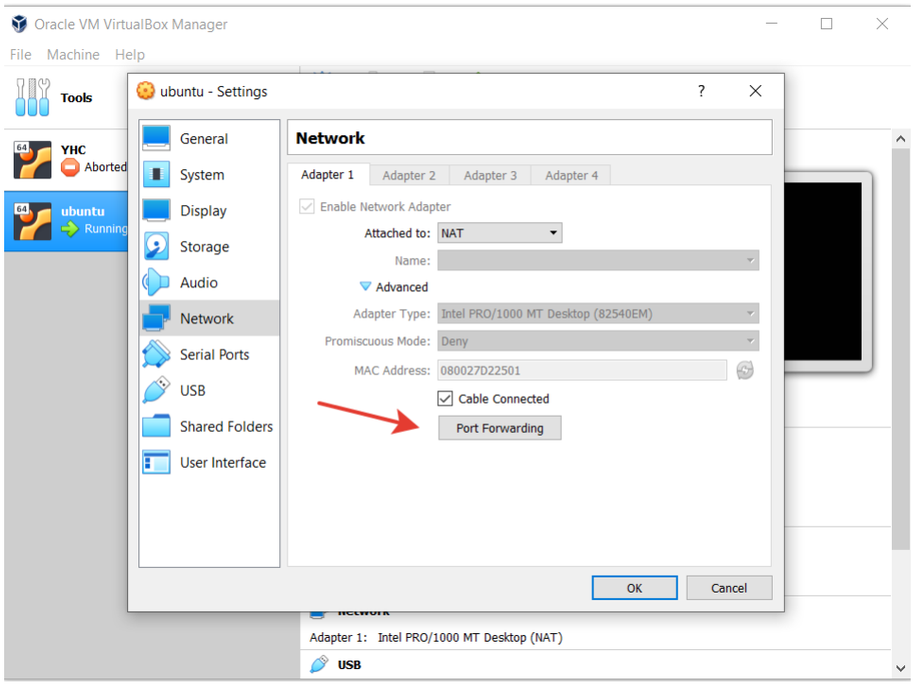
```
HiddenServicePort 2023 127.0.0.1:2023
HiddenServiceVersion 2
```

Peki bütün bunlar ne anlama geliyor?

HiddenServiceDir başlatılan servis ile ilgili ayarlarımızın ve adresimizin olacağı dizin. Bu dizin çok önemli aşağıda ayrıntılara yer vereceğiz.

HiddenServicePort talimatı ile TOR'un 2023 numaralı portu dinlemesini ve 127.0.0.1 adresindeki 2023 numaralı porta istekleri yönlendirmesini istiyoruz.

Hayda! Hani sanal makinede idi sunucumuz? Evet ama endişelenmeyin! Şimdi loopback adresimize, yani 127.0.0.1'in 2023 numaralı portuna gelen isteklerin NAT arkasındaki 10.0.2.15 'in 2023 numaralı portuna yönlendirilmesi için küçük bir ayar yapacağız. Bu ayar VirtualBox üzerinden sanal makinemize bir port forwarding yani port yönlendirme ayarı tanımlamaktan ibaret. Virtualbox'ta ilgili sanal makinemizin networking ayarlarından bu işlemi gerçekleştireceğiz:



Bu işlemlerden sonra sanal makinenizi yeniden başlatmalısınız.

Şimdi Nginx sunucumuzda da 2023 numaralı portu dinlemesine dair bir ayar yapmamız gerekiyor. Ayrıca bir de web sitemizin adresini bilmemiz lazım ki Nginx'in *servername* ayarını da yapıp, sadece bu Host bilgisi ile gelen isteklere yanıt vermesini sağlayabilelim.

Benim web site adresim nedir?

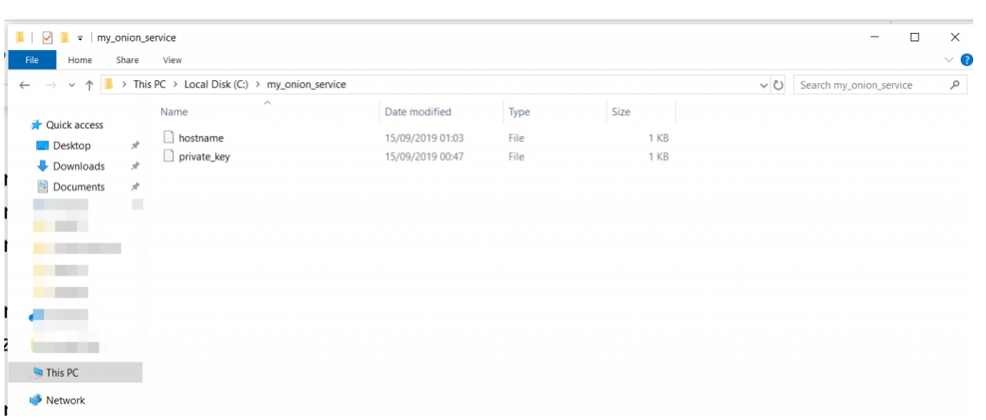
torrc dosyasına üç satır eklemiştik:

```
HiddenServiceDir C:\my_onion_service
HiddenServicePort 2023 127.0.0.1:2023
```

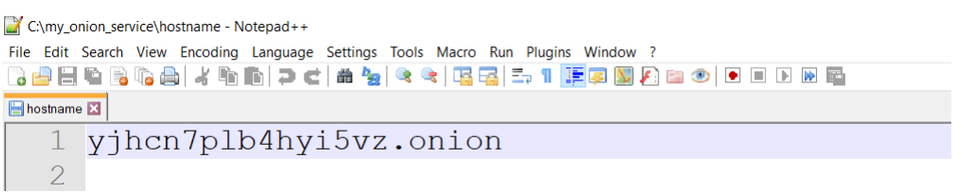
HiddenServiceVersion 2

HiddenServiceDir dizini kritik bir dizin. Web sitemize Onion Servis tarafından atanan domain name'i öğreneceğiz.

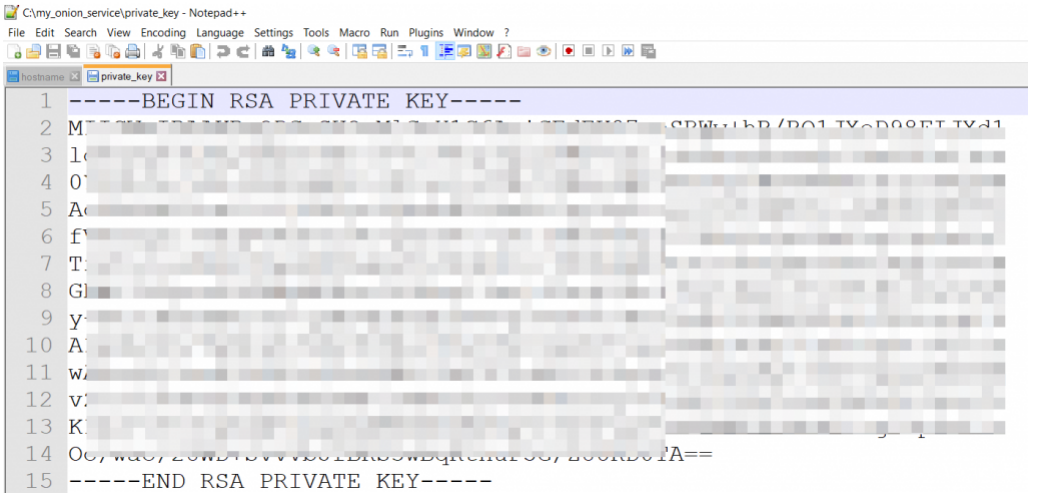
HiddenServiceDir dizini iki adet dosya içeriyor: *hostname* ve *privatekey*



Bu dosyalar torrc dosyasındaki talimatlar doğrultusunda Tor servisi başlatıldığında hazırlandı. hostname dosyası bir sürpriz bilgi içeriyor; müstakbel web sitemizin adresini:



yjhcn7plb4hyi5vz.onion Dağlara taşlara! Bu nasıl adres böyle? Bu adres aynı dizinde bulunan private_key yani web sitenize erişim için gerçekleşecek olan uçtan uca şifrelemenin private_key'i kullanılarak hazırlandı.



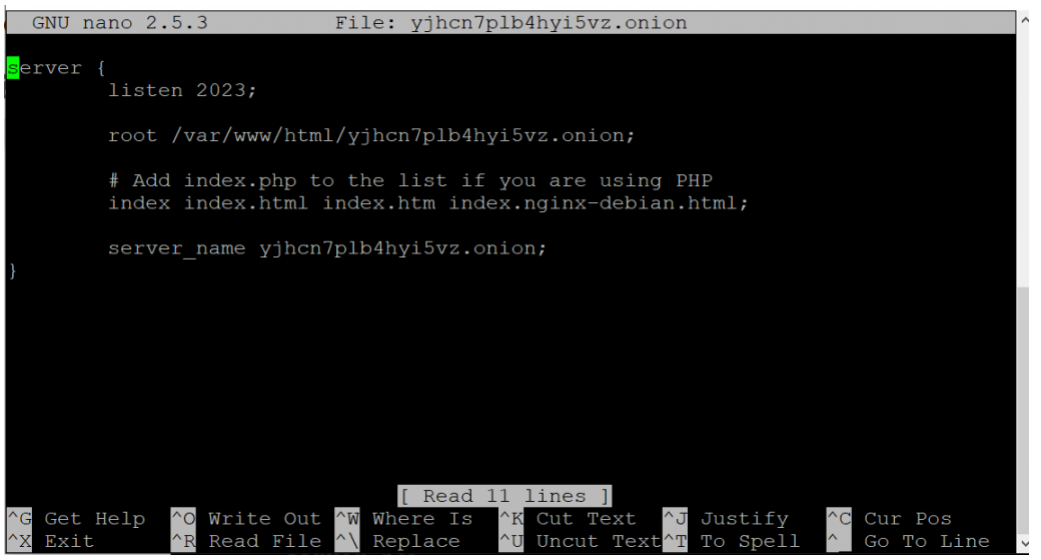
TOR servisi öncelikle oluşturulan bu private key'den extract edilen public key'in SHA1 ile özetini aldı. Bu özetin ilk 80 biti alınarak ve base32 encoding ile encode edilerek 16 karakter uzunluğundaki bu adrese ulaşıldı.

Buradaki mekanizma harikulade tasarlanan bir mekanizma. Domain name'iniz doğrudan public key ile ilişkili olduğu için bir nevi domain name üzerinden self-signed bir sertifika kullanmış oluyorsunuz.

SHA1 gibi özet algoritmasını görüp, haklı olarak yüzünü buruşturan okurlar için küçük bir izahat: Version 2 kullanarak hazırladığımız bu Onion Service'in 3. Versiyonunda daha güçlü algoritmalar ve daha uzun adresler sizi bekliyor. Konunun ayrıntılarına TOR'un web sitesinden ulaşabilirsiniz.

Web sitemizin adresini öğrendiğimize göre şimdi Nginx sunucumuzu konfigüre etmemiz için her şey hazır!

/etc/nginx/sites-available dizini altında sitemizin adını taşıyacak bir dosya oluşturuyoruz: yjhcn7plb4hyi5vz.onion



Şimdi bu dosyayı *sites-enabled* isimli klasöre taşımamız gerekiyor:

```
sudo cp yjhcn7plb4hyi5vz.onion ../sites-enabled/
```

Ayarlardan sonra Nginx sunucusunu restart etmeyi unutmayın:

```
/etc/init.d/nginx restart
```

Web sitemize TOR Browser'ı kullanarak *yjhcn7plb4hyi5vz.onion* adresi üzerinden erişilebilir!

Şimdi sorulara geçebiliriz.

Daha güzel bir domain ismine sahip olabilir miyim?

Evet daha okunaklı -TOR literatüründe buna vanity domain deniyor- bir domain'e sahip olmak mümkün. Örneğin Facebook'un Onion Service adresi facebookcorewwwi.onion

Yazının başlangıcında Onion Service domain adının private key'den extract edilen public key'in SHA1 özetinin alınması ile başlayan bir süreç olduğunu söylemiştim.

Eğer güçlü bir CPU'ya sahipseniz, RSA anahtar çiftlerini üretip, SHA1 özetini alıp, sonra base32 ile encode edip, ilk 16 karakterin arzu ettiğiniz domain name'i içerip içermediğini kontrol edebilirsiniz.

Bunu servis olarak sunan siteler de mevcut. Fakat bendeniz bu sitelerin kullanılmasını tavsiye etmiyorum. Zira siteniz için hayati önemde olan private key-public key değer çiftinin üretilmesini işlemini başka birine havale etmiş olacaksınız. Dolayısıyla bu key'lere sahip olan biri domaininiz üzerinde sahiplik elde edebilir.

Sisteminizin erişilebilir olması, tıpkı diğer web sayfaları gibi hosting'in yani web sitesi dosyalarını host ettiğiniz bilgisayarın ayakta ve çevrim içi olmasına bağlı. Diğer sitelerden farklı olarak TOR servisi de başlatılmış durumda olmalı.

Onion Servisler aracılığı ile sadece web sitesi diğer SSH vb. Üstelik NAT arkasındaki servisleri de erişime açabilirsiniz.

Onion Servisleri çok kullanışlı özellikler sunuyor. Mutlaka version 3'e bakmanızı öneriyorum. Ayrıca güvenlik bahsi bu yazının limitlerini aşmış durumda. Web sitesini izole bir makine üzerinde çalıştırıyor olmanız en önemli adımlardan biri. Fakat tek başına bu adım yeterli değil. Mutlaka sunucu güvenliği konusunda da dökümanlara göz atılmalı, örneğin HTTP response'unda sunucu bilgilerinin ifşa olmasını engellemek için gerekli konfigürasyon ayarları yapılmalıdır.

Domain'imi bulmalarını nasıl sağlayabilirim?

TOR Network'üne adım atanların ilk duraklarından biri olan The Hidden Wiki gibi dizin servislerine web sitenizi kayıt edebilirsiniz.

.onion uzantılı web siteme normal tarayıcılar da erişebilecek mi?

Bu cevaba hem evet hem de hayır yanıtı verebiliriz. Yazının başlangıcında TOR'un işletim sisteminde bağımsız bir servis olarak nasıl başlatılabileceğine değinmiştik. Şayet tarayıcı SOCK üzerinden Proxy olarak TOR için ayarlandı ise sitenize erişebilir.

Ama pek çok durumda, DNS Leakage, web sitelerine erişim için TOR Network'ü kullanılsa da adres çözümleme için ISP'nin yani servis sağlayıcınızın DNS sunucularına işletim sistemi tarafından müracaat edilecektir. Bu DNS sunucuları da maalesef .onion uzantılı domainleri çözümleyemeyecek, dahası hangi siteye erişmek istediğinize dair bilgiyi ifşa etmiş olacaksınız.

Daha fazla insan TOR kullandığında, hatta bu iş için donatılan TOR Browser'ı kullandığında böylesi ihtimaller sorun olmaktan çıkacaktır.

Yazının, bilgi ve düşüncenin özgürce üretilip, paylaşılabilmesi çabalarına mütevazi bir katkı olarak değerlendirilmesini arzu ediyorum.

Bilgi güçtür!

82 Shares 66

© ARKA KAPI DERGİ 2020.
Sesini çıkarmak isteyen bir grup insan tarafından yapıldı.