Özgürlük

Eşitlik

Kardeşlik

Ya istiklal ya ölüm

Her şey tam bağımsız Türkiye için!

Hosts

Duydum ki…

Engellemeye çalışıyormuşsun…
Duydum ki…
TIB vatandaşımın haber alma özgürlüğünü kısıtlamaya çalışıyormuş!

Ben…
Önder Gürbüz, 25 senelik meslek hayatımda (öğrenim zamanımı dâhil bile etmiyorum)…
Bilişimden başka bir şey yapmamışım…
Bilişimin her dalında…
Programlamadan, platin tamirine, LAN, WAN, MAN ve GAN ağıları kurarak…
Güvenliğini üstenmişim…
Sen ve TIB mi beni durduracak?

Akılına şaşarım…
Sen bizi yandaşın, yoldaşın mı sandın?
Sen bizi trafolara giren / girebilen…
Kedilerden daha mı akılsız sanıyorsun?

Bugün…
Engellemeleri nasıl aşacağınızı…
Bizlerin dilinde Hijacking denen - yanlış yönlendirmeyi – nasıl aşacağınızı açıklayacağım!

Elimden geldiği kadar basit bir dil ile anlatmaya çalışacağım…
Önce bir tespit ile başlayalım (Windows işletim sitemi için geçerlidir. Çoğunluk bu sistemi kullandığı için yine onun üzerinden anlatacağım):

Kendi bilgisayar ayarlarınız (yani admin tarafından yapılan ayarlar) diğer ayarların üstündedir!

Bu ne anlama geliyor daha sonra anlayacaksınız. Bu olguyu anlatmakla vakit kaybetmek istemiyorum. Birçoğunuzun bildiği üzere DNS ayarlarıyla oynandığında engellenen sayfalara ulaşılabilmektedir. Peki, DNS nedir?
DNS sistemi insanların işini kolaylaştırmak için işleme konan bir sistemdir. Dikkat burasını anlamanız şart: Yani internet tarayıcısına (http://www.) google.com yazdığınızda, DNS sunucusu tarafından alan adı (google.com) dünya çapında yalnız bir kez olan IP numarasına (mesela google.com'un ip numaralarından biri olan 173.194.116.97) çevrilir. Şimdi taktir edersiniz ki Google.com'u, 173.194.116.97'den daha kolay aklınızda tutabilirsiniz. İşte bu yüzden DNS'ler vardır. Root DNS denen bir avuç DNS'ın yanı sıra binlercesi vardır ve 24 saat içeresinde birbirleriyle defalarca irtibata geçerek kendilerini güncellerleler. Buna rağmen bazen bir alan adının dünya çapında tanınması 6 ay kadar sürebilir. Ayrıntısına girmeyeceğim ama bu yöntemin dezavantajda tam budur. Bu yöntemi kullanabilirsiniz çünkü hiç bir ayar değiştirmeden – doğrudan – ilgili sunucu ile irtibata geçtiğinizden, DNS ilk etapta devredişi kalır. Çünkü bu yöntemi kullandığınızda Root DNS'ler sizi doğrudan ilgili sunucuya yönlendirecektir. Yani siz Türk Telekom veya başka bir Türk DNS ile irtibata geçmeden doğrudan veya bunlar tarafından - siz anlamadan - yanlış yönlendirmeye (Hijacking) tabii tutulamadan istediğiniz adrese ulaşmış oluyorsunuz.

Mesela:
http://173.252.110.27 diye tarayıcınıza yazdığınızda Facebook açılacaktır.
http://173.194.35.133
173.194.35.128
173.194.35.132
173.194.35.129
173.194.35.136
173.194.35.130
173.194.35.131
173.194.35.142
173.194.35.134
173.194.35.137
173.194.35.135 Google IP numaralarından bazılarıdır. Burada bir parantez açarak bir bilgi daha vereyim; Google IP numaralarından herhangi birini alarak ardına YouTube yazdığınızda ne açılacak bilin bakalım? (http://173.194.35.142/youtube)
Ancak…
http://199.16.156.230 yazdığınızda Twitter açılmayacaktır. Çünkü öyle görünüyor ki Twitter sanal bir IP numarasına sahiptir (yani diğer örneklerde olduğu gibi gerçek bir IP numarasına sahip değildir. Bunun nedeni ise eskilere dayanır. Yeri geldiğinde anlatırım).

Bu kadar basit mi?

☺ Maalesef değil!

Bu yöntem büyük siteler için, yani kendi gerçek IP numarasına sahip siteler için geçerlidir (Bazen onlarca alan adı aynı IP numarasını paylaşabiliyor ve bu ilgili sunucu tarafından yönetiliyor). Ama üzülmeyin hepinizin kullanabileceği basit başka çözümlerde var.
Konuyu daha fazla açmadan sizin "bildiğiniz" yöntem ile devam edelim; Birçoğunuz DNS numarasını IP ayarlarına veriyorsunuz. Peki, kaçınızın alternatif DNS sunucusuna dikkat ederek oraya bir DNS sunucusunun IP numarasını yazdı?
Bilgisayarınız ağ işlemlerinde öncellikle sistem içinde (yani kendi ayarlarında) gerekli komutlar, güvenlik düzenlemeleri gibi ayarların varlığına bakar, sonra gerektiğinde başka bir "üst" sistemden ayar alabilir miyim diye ağ içinde arama yapar.

Örnek: DNS sunucusu: 194.25.2.129 Alternatif sunucu 8.8.8.8 gibi!

Yine bazı Router'ler DNS ayarlama imkânı sunmaktadır. Sizin yerinizde olsam kendi bilgisayarımda DNS, alternatif başka bir DNS sunucusu ve imkan varsa Router'de – farklı – DNS numaralarını kayıt ederdim. Nedeni de – tekrarlamakta – fayda var; bilgisayarınızın öncelliği kendi ayarlarına önem vermesidir.

Gelelim Tayyip ve TIB diktatörlüğüne karşı vuracağımız öldürücü darbeye. Bu yöntem Personal Computing'de eski bir "kurt" olup olmadığınızı gösterir. Çünkü "genç" bilişimciler bu ve buna benzer birçok yöntemi bilmez(!?)
Anlatacağım bu yöntem gerçekten çok eskilere dayanır ve Windows ve Unix (yani sizin kullandığınız ve Unix sistemine dayalı Linux içinde geçerlidir).

Takdir edersiniz ki…
Internet kurulduktan ve PC'ler piyasaya arz edilmeye başladıktan sonra DNS'ler az sayıda mevcuttu. Ve tabii fiyatlar çok ama çok yüksekti (ben profesyonel olarak bu işe başladığımda bir bilgisayar 30.000 Mark'tı. Aşağı yukarı Efsanevi 8086 işlemci piyasaya çıktığından beri bilişim ilgi alanımdaydı ve bu ilgi malulen emekli olmama rağmen hala sürmektedir) …

İşte o günlerden bugünlere kadar gelebilen bir dosya (tüm Windows, MAC OS ve Linux sürümlerinde mevcut olan) ile Tayyipgillerin münasip bir tarafına tekme atabilirsiniz. Nasıl mı? Anlatayım efendim, ancak…
Bundan sonrasını hayata geçirebilmeniz için – mutlaka – bilişimden – iyi - derecede anlayan birisini yanınıza almanız lazım çünkü nasıl yapıldığına dair pek ayrıntısına girmeyeceğim. Mutlaka bilmeniz gereken ile yetineceğim. Nedenine gelince, başka türlüsü bu makalenin gerçekten sınırlarını zorlar. Geçelim…
Bu dosyanın adı, hosts veya lmhost olarak geçer ve bir text (txt) dosyasıdır. Yani üzerine tıkladığınızda Windows hangi programla açayım diye sorduğunda sisteminizde mevcut bir editörü seçeceksiniz (notepad gibi). Bu dosyanın görevi yukarıda anlatılan DNS sunucularının görevini üstlenmekti.

Ama dikkat! Bu dosya gerekli önlemler alınmadığında bazı (az sayıda) kötü amaçlı kişiler tarafından sizi yanlış yönlendirmeye kullanılmaktadır. Alınması gereken önleme daha sonra değineceğim.

Neyse,
Öncellikle, bundan sonra yapacağınız tüm işlemleri admin olarak yapmaya özen gösterin ve adı geçen bu dosyayı görebilmeniz için Explorer ayarlarında tüm dosyaları görebileceğinizi sağlamanız gerekiyor. Windows XP'den Windows 8.1'e kadar (önceki sürümlerde de bu dosya mevcut ama ilgilenen yerini kendi araştırsın. İşletim sistemleri çok eski olduğundan burada bunlara değinmeyeceğim) bu dosyayı %SystemRoot%\System32\Drivers\Etc
(yani \windows\System32\Drivers\Etc) dizini altında bulabilirsiniz. Host dosyasının noktadan sonra eklentisi yoktur. Dosyayı açtığınızda muhtemelen şöyle bir içerik ile karşılaşacaksınız:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
```

```
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

işaretini not almak için kullanabilirsiniz. #'den sonra gelen herhangi bir şeyin bir işlevi yoktur.

Ben sizin için bu dosyayı düzenleyerek download için hizmetinize sunacağım. Olur ya ileride sizin için önemli başka yasaklı siteler gelebilir. Bu dosyayı yeniden düzenleyerek kayıt etmeniz yeterli olacaktır.
Tekrarlamakta fayda var: Bu dosya sayesinde IPS'lerin DNS ayarlarından etkilenmeden dosyanın içeriğinde bulunan sitelere ulaşabilirsiniz. Çok önemli hosts dosyasının bir eklentisi yoktur!!!
Hatırlı okuyucularım bilirler, defalarca tekrarladım, buradan bir kez daha tekrarlamak istiyorum insanların iyiliği için düşünülmüş herhangi bir olgu, insanların aleyhinde de kullanılabilir. Bu açıdan alınması gereken ek önlemlere de kısaca değinmek istiyorum. Ayrıntılara girmeyeceğim.
1. Host dosyası işlendikten sonra (Türkçesini bilmiyorum) mutlaka write protect olarak kayıt edilmeli ve değişikliğin tarihi bir yere yazılmalı. Arada bir tarihe bakılmalı ki siz istemeden / bilmeden bir değişikliğe uğrayıp uğramadığını anlayın.
Not: Hackerler veya devlet kurumları, bilgisayarınızda yeterli güvenlik önlemi almadığınız taktirde bu dosyayı değiştirerek sizi "yanlış" yönlendirebilirler.
2. Mutlaka bir anti virüs kullanın (Microsoft'un anti virüs yazılımı ücretsizdir. Buna rağmen görevini iyi derecede yerine getiriyor)
3. Her şeye, tüm aldığınız önlemlere rağmen birileri sisteminize girmeyi başarabilir bunun için arada sırada; mesela Hijack This gibi bir yazılımı kullanmayı ihmal etmeyin.

Tarafımdan güncellenmiş host dosyası

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

81.169.145.157          www.gurbuz.net
173.194.32.242          www.google.com
173.194.35.130/youtube  www.youtube.com
199.16.156.198          www.twitter.com
173.252.110.27          www.facebook.com
192.155.212.202         www.whatsapp.com
```

204.79.197.200	www.bing.com
213.180.204.62	www.yandex.com