~ BU KİTABI ÇALIN ~

II

Bu Kitabı Çalın – II

Haziran 2014

Teşekkür

Bana ve yazdığım yazılardaki eksiklerime rağmen hoşgörülü davranan değerli dostlarıma teşekkürlerimi sunarım.

İçindekiler

Giriş

Kame projesini oluşturup yazılar yayınlamaya başladığımda şu anki içeriği oluşturabileceğim aklımın ucundan dahi geçmiyordu. İçerik bir yana, bu içeriği oluşturabilmek için harcadığım süre ve güç için kendime şaşırdığım bile oluyor. Bu noktaya kadar gelebildiğim ve ikinci sayıyı yayınladığım için çok mutluyum.

Bu Kitabı Çalın – II sayısı Kame'nin Ocak – Haziran ayları arasında yayınlamış 25 adet yazısını içermektedir. Yazılar içerik itibariyle, 5651, sansür, gizlilik, URL tabanlı engelleme, kriptografi, anonimlik araçları ve güncel güvenlik konularından oluşmaktadır. İlk kitapda görmüş olduğunuz üzere yazılarda atıflarda bulunulmuş ve kaynak gösterimi olarak dipnot tercih edilmiştir. Dipnotlarda verilen bağlantılar zaman içinde kırılabilir veya silinbilirler. Bu konuda benimle iletişime geçerseniz memnun olurum.

Son olarak, bu kitap bir derleme veya kolektif bir grubun ortaya çıkardığı bir şey değildir. Tüm yazılar ve GNU/Linux canlı CD projesi tek bir kişiden çıkmaktadır. Yayınlamış olduğum iki kitap ve bir özel sayı ile ilgili görüşlerinizi bildirmekten lütfen çekinmeyin.

1. Bilim Etiği, 5651 ve Sansür

Amacım bilimsel araştırmalarda gerçeğe uymayan yanıltmalara yönelik sorunların ve bu konularda uyulması gereken etik kurallarının saptanmasından ziyade, Internet sansürünün genel anlamıyla bilim etiğini nasıl ve hangi yönde etkilediğini tartışmaktır.

İlk önce kavramları kısaca açıklayarak ilerleyeceğim. Araştırma, araştırmacıların doğru bilgiye ulaşmak için yaptığı eylemlerden oluşan bir süreci ifade eder. Bunu hepimiz hayatımızın birçok alanında gerçekleştirmekteyiz. Ayrıca, Internet günümüzde araştırma eylememizin en büyük halkasıdır. Bununla birlikte, araştırmacılar alanlarında "**özgürce**", planlı ve sistemli olarak veri toplar, analiz yapar, yorumlar, değerlendirilmesi ve geliştirilmesi için başkalarının da incelemesine ve kullanmasına izin verir. Buna, araştırmacılıkta bilim etiği denir.

Araştırmacılıkta bilim etiğine en uygun örneklerden biri GNU/Linux'tur. GNU/Linux'u herkes ücretsiz olarak indirebilir ve kullanabilir. Fakat, GNU/Linux ile Windows arasındaki en önemli fark, ticari yazılım modelinden ziyade GNU/Linux'un "**açıklığıdır**". Bilim etiğinde de söylediğim gibi nasıl ki veriler incelenmesi, kullanılması ve geliştirilmesi için başkalarının da kullanmasına ve geliştirmesine sunuluyorsa, aynı şekilde GNU/Linux da sunulmaktadır. Ayrıca, açık kayak modelin bilim adamları tarafından seçilmesinin nedeni sadece etik değil, bilimsel bilgiye ulaşmanın en başarılı yolu olmasıdır[1].

1 Himanen, Pekka. (2005). Hacker etiği. İstanbul: Ayrıntı Yayınları.

17 Aralık 2013 yolsuzluk operasyonu[2] ile başlayan yeni süreçten sonra bilgiye açık erişim için Internet en yoğun kullanılan, bilginin incelenmesi, kullanılması, değerlendirilmesi ve yeniden paylaşılması için en etkin ortamdı. Bunu sadece yolsuzluk operasyonu ile sınırlandırmıyorum. Fakat, AKP Şanlıurfa Milletvekili Zeynep Karahan Uslu[3], "**5651SayılıKanun'nda değişiklik teklifimiz toplumsal ihtiyaçlar&özgürlükler dengesi hassasiyetleGÖZETİLEREKhazırlandı**" tweet'i ile 5651 S. Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[4] değişikliği talebinde bulmaktadır. Değişiklik son olarak torba kanun tasarısı içine de taşındı[5]. Bu tasarının zamanlaması ise Internet'in açık bilgi akışındaki rolü açısından çok önemlidir.

Tasarının içeriği, Internet sansürünün kapsamını daha da çok artırmaya, daha keskin ve sert kurallarla Internet'teki ifade özgürlüğünü kısıtlamaya yöneliktir. Şunu iyi anlamak lazım; Internet özgürlüğü ifade özgürlüğünün koruyucusudur. Çünkü, araştırmacılık bulguların ifade edilmesini ve özgürce paylaşılmasını da gerektirir. Eğer siz, kendinizi özgürce ifade edemiyorsanız araştırma özgürlüğüne de sahip olamazsınız. Bu, doğrudan açık bilgi akışını etkiler. Açık bilgi akışında bahsettiğim verilerin analizi, değerlendirilmesi, başkalarına sunulması, geliştirilmesi ve yeniden sunulması döngüsü etkilenecek, döngü içerisindeki aşamaların bir kısmı ya da tamamı sansürden dolayı etkilenmiş/engellenmiş olacaktır.

---

2 http://t24.com.tr/listeler/bugun-baslayan-yolsuzluk-operasyonuna-dair-tum-haberler
3 https://twitter.com/zkarahanuslu/status/413423658326315008
4 http://web.tbmm.gov.tr/gelenkagitlar/metinler/266126.pdf
5 http://t24.com.tr/haber/internet-yayinciligina-agir-denetim-ve-yaptirimlar-geliyor/247549

Internet özgürlüğü, ifade özgürlüğü, açık bilgi akışı, bilim etiği gibi haklar ve süreçler girifttir. Sizin bunlardan herhangi birine uygulayacağınız sansür diğerlerini de doğrudan ve olumsuz yönde etkilemektedir. Günümüzde en etkin araştırma yöntemi Internet'te kaynak taramasıdır. Ayrıca, içeriklere rahat ve sansürsüz erişimden, test ve bulguların Internet'te paylaşılmasından ve tartışılmasından geçer. Açık bilgi akışının, şeffaf, sansürsüz ve herkesin erişimine izin vermediği durumlarda bilimin ve toplumun ilerlemesi söz konusu dahi olamaz.

Sonuç olarak ısrarla vurguladığım şey; Internet muktedirin keyfiyetine, kendi çıkarlarına ve kendisini kormaya yönelik bir süzgeçten geçirilemez. Internet özgürlüğü ve erişimi bir insan hakkıdır. Bu hak, birçok hakla girift haldedir ve birçok hakkın koruyucusudur. 21. yüzyılın toplumsal sorunları daha çok artmış ve daha karmaşık bir hal almıştır. Her alanda yaşanan yozlaşmalara çözüm olarak etik kavramı ortaya çıkmıştır. Bilim etiğinin kendi iç sorunları dışında bir de Internet özgürlüğüne vurulacak darbe ile uğraşmak zorunda kalması, bilimsel gelişimi yavaşlatır ve hatta durdurabilir. Bu, her toplum için kabul edilemez bir durumdur.

Korsan Parti Bildirisi[6]

Higgs Bozonu'nun Keşfinde GNU/Linux[7] (*Murat'a teşekkürler!*)

6 https://docs.google.com/document/d/1DnVkX_bNh9o1cF89Is0rBU9UR7l5-hEy3XqlJkog-Fg

7 http://www.nemedya.com/gunluk/higgs-bozonunun-kesfinde-gnulinux-ve-ozgur-yazilimlar-kritik-bir-rol-oynadi

2. DNSCrypt

Veri trafiğini daha iyi şifrelemenin en iyi yollarından biri de DNSCrypt kullanmaktır. Sizleri küresel dinleme ve yapacağınız hatalardan korumayacak ama DNS trafiğiniz şifreli bir hale dönüşecektir.

DNSCrypt[8] kısaca, bir istemci ile DNS çözücü arasındaki iletişimi şifreleyen bir araçtır. Diğer bir deyişle, DNSCrypt proxysi doğrudan yerel çözücü olarak kullanabileceğiniz ya da DNSCrypt protokolü olarak DNS isteklerini gönderen, şifreleyen ve doğrulayan yerel bir servis sağlamaktadır. Bununla birlikte, DNSCrypt yüksek hızlı ve yüksek güvenlikli elliptic-curve kriptosu[9] kullanmakta ve istemci ile birinci-seviye çözücü arasındaki iletişimi korumaya odaklanmaktadır.

DNSCrypt'i bu kadar farklı kılan şeylere bakarsak eğer, SSL[10] nasıl HTTP web trafiğini HTTPS şifreli web trafiğine çeviriyorsa DNSCrypt de sıradan bir DNS trafiğini şifreli DNS trafiğine dönüştürmektedir. Bu da kullanıcıya dinleme ya da man-in-the-middle saldırıları gibi durumlarda koruma sağlamaktadır. Ayrıca, DNSCrypt platform bağımsız bir uygulamadır ve GNU/Linux, Windows ya da iOS (*jailbreak şartı var*) sistemlerde rahatlıkla kullabilirsiniz. Örneğimiz GNU/Linux üzerinde olacak fakat sizler farklı platformlar için en altta verilmiş bağlantılar üzerinden hareketle gidebilirsiniz. Bununla birlikte, dağıtımınızın ne olduğunu bilmiyorum. Eğer, kullandığınız dağıtımın depolarında dnscrypt paketi yok ise direkt 2. yönteme

8 http://www.opendns.com/technology/dnscrypt/
9 https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
10 https://en.wikipedia.org/wiki/Secure_Sockets_Layer

bakabilirsiniz.

2.1. Depodan Kurulum

İşlemlerimizi terminal üzerinden root olarak gerçekleştireceğiz. Hemen bir tane açın ve:

kame ~ $ apt-get install dnscrypt-proxy (*pacman -S dnscrypt-proxy veya dağıtımınız neyse onun paket yöneticisi ile kurulumu gerçekleştirin.*)

Kurulum tamamlandıktan sonra dnscrypt-proxy servisini başlatın. Debian ve türevi dağıtımlarda bu otomatik olarak gerçekleşecektir. Eğer başlamazsa:

kame ~ $ /etc/init.d/dnscrypt-proxy start

systemd kullanan farklı bir dağıtımda:

kame ~ $ sysyemctl enable dnscrypt-proxy

kame ~ $ systemctl start dnscrypt-proxy

yaparak başlatabilirsiniz.

2.2. Elle Kurulum

Eğer depolarınızda yok ise aşağıdaki adımları gerçekleştirin.

kame ~ $ wget -c http://download.dnscrypt.org/dnscrypt-proxy/dnscrypt-proxy-1.3.3.tar.gz

kame ~ $ tar xzf dnscrypt-proxy-1.3.3.tar.gz

kame ~ $ cd dnscrypt-proxy-1.3.3

kame ~ $ ./configure

kame ~ $ make

kame ~ $ sudo make install

Bu aşamaların herhangi birinde (*make install hariç*) hata alırsanız mevcut hatayı aratarak eksik kütüphane veya paketleri kurmanız gerekebilir.

2.3. Kullanım

Kurulum aşamalarını tamamlamış iseniz artık kullanıma geçebiliriz. Statik IP ayarları yaparak kullanımını göstereceğim. Sadece DNS sunucusuna yazarak da kullanabilirsiniz. Seçim size kalmış.

kame ~ $ sudo ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.3 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::52e5:49ff:feda:8b5a prefixlen 64 scopeid 0x20

ether 50:e5:49:da:8b:5a txqueuelen 1000 (Ethernet)

RX packets 345058 bytes 405146897 (386.3 MiB)

RX errors 0 dropped 8 overruns 0 frame 0

TX packets 231282 bytes 53324829 (50.8 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Görüldüğü üzere eth0 kullanmış olduğum bağlantım. inet değeri ise bilgisayarımın ip'si. Ağ yöneticiniz NetworkManager veya başka bir şey olabilir. Ağ yöneticinizinde düzenlemek üzerekullandığınız bağlantıyı (*eth0, wlan0 vs.*) açın (*örneğin Edit connections -> Ethernet (eth0) -> Edit -> IPv4 Settings*) ve:

Adress: 192.168.1.3

Netmask: 255.255.255.0

Gateway: 192.168.1.1

şeklinde düzenleyin. Son olarak DNS Servers (*DNS sunucusu*) kısmına 127.0.0.1 yazın, kaydedin ve ağ yöneticinizi tekrar başlatın. 127.0.0.1, bizim yerel DNSCrypt proxymizdir. Bundan sonraki süreçte artık trafiğimiz şifreli bir şekilde akmaya başlayacaktır.

Dikkat etminiz gereken en önemli nokta DNSCrypt erişime engelli siteleri aşmak için bir araç olmadığıdır. Veri trafiğini en iyi şekilde şifrelemeye çalışmakta fakat bu süreçte IP'niz gizlenmiyor, yeriniz değişmiyor, Internete çıkış noktanız farklılık göstermiyor. Bunu kesinlikle aklınızdan çıkarmayın. Diğer platformlar için indirme

bağlantıları aşağıdadır:

- Windows
- iOS
- Android

3. Fişlemeyi Normalleştirmek

> *Özellikle iktidarın devamlı ihbar edin çıkışları, son bulacağını söyledikleri fişmele ile doğrudan çelişmektedir. Epey deneysel bir yazı oldu. Bir eleştiri yazısı olarak yorumlarınızı beklerim.*

Gezi sürecinden bildiğimiz üzere insanlar Gezi'ye destek vermek amacıyla geceleri ülkenin birçok ilinde "**tencere tava**" çalmaya başlamıştı. Çok geçmeden Erdoğan; "**Komşuyu rahatsız etmek suçtur. Ben değil yasalar söylüyor. Müracaatınızı yapacaksınız, yargıya bildireceksiniz.**" diyerek tencere tava çalanların ihbar edilmesini istemişti[11]. Ardından, bu konuyla ilişkin olarak "**Sırdaş Polis İhbar Noktası**" projesinden bahsetmişti[12]:

Mahalle aralarına yerleştirilecek bu sistem sayesinde, bir suç işlendiğinde, insanlar 'kimliğim tespit edilir mi?' endişesi yaşamayacak. Bu sistem ile ister yazılı olarak, isterse de sesli olarak bu kutulara ihbarda bulunabilecek. **Bu kutulara yapılan ihbarlar ise kesinlikle gizli kalacak.** Projenin kısa bir zaman diliminde başlatılması hedefleniyor.

Görüldüğü üzere yazılı veya sesli olarak mahalle aralarına yerleştirilmiş bu sisteme insanlar kimlikleri gizli kalacak şekilde ihbarlarda bulunabilecekler. Ek olarak, bu proje sayesinde "**polise olan ihbarların artırılması ve ihbar sisteminin işlevlik kazanması**" amaçlanmakta olduğu söylenmiştir. Bir süre sonra, gündem değiştirme

11 http://siyaset.milliyet.com.tr/faiz-lobisi-niye-hopluyor-/siyaset/detay/1739099/default.htm
12 http://www.bianet.org/bianet/insan-haklari/149020-tencere-tava-calan-komsusunu-ihbar-eden-oldu-mu

gücünü iyice kaybeden Erdoğan'ın kızlı-erkekli öğrenci evleri çıkışı[13] olmuştu. "**Üniversite öğrencisi genç kız, erkek öğrenci ile aynı evde kalıyor... Vali Bey'e bunun talimatını verdik. Bunun bir şekilde denetimi yapılacak.**" demişti. Bu söyleminden sonra epey tepki çekmiş, kızlı-erkekli öğrenci evlerinin ihbarı başlamış[14], kendilerini ihaber edenler olmuş ve ihbar sonucunda da bir kişi hayatını kaybetmişti[15]. Görüldüğü üzere her iki söylemin de ortak yönleri; neyin suç olduğunun bir kişi tarafından belirlenmesi ve "**ihbar.**"

Bu sefer çok yakın bir tarihte, 6 Aralık 2013'te "**Trafikte Yeni Dönem! Herkes Polis Olabilecek**" başlıklı yeni bir haber yayımlandı. Ayrıca, bu haber tv programlarında da gösterildi. Haberde geçen bölümden bir altıntı yapayım:

Tasarı Meclis'ten geçerse elinde kameralı cep telefonu bulunan herkes trafik casusluğu yapabilecek. Vatandaş aşırı hız, kırmızı ışık ihlali, emniyet kemeri, yasak park, araç kullanırken cep telefonu ile konuşma, hatalı sollama, araçtan sigara izmariti, çöp atma gibi eylemleri ya fotoğraflayarak tespit edecek ya da videoya çekecek.

Alıntıdan da görüldüğü üzere insanlar ellerindeki cep telefonları ile isterlerse trafik casusluğu yapabilecekler. Yani tekrar aynı bahaneyle, yasalara aykırı bir durumun ihbar edilmesi istenmektedir. Bununla birlikte, "**casusluk**" kelimesi "**Sırdaş Polis İhbar Noktası**" projesi ile -*bence*- doğrudan ilişkilidir. Çünkü, her ikisinin de ortak

13 http://haber.sol.org.tr/devlet-ve-siyaset/erdoganin-freni-patladi-kiz-erkek-ogrenci-ayni-evde-kaliyor-denetleyecegiz-haberi-
14 http://www.hurriyet.com.tr/gundem/25110166.asp
15 http://www.cnnturk.com/turkiye/-kizli-erkekli-ev-tartismasi-korkusu-oldurdu

noktası kimlik gizliliğidir (*e-posta ile ihbar bu konuda biçilmiş kaftan*). Şimdi bir ayrım yapalım. Mobese, devletin kendi eliyle koyduğu bir gözetleme sistemidir. Haberlerde insanlara "**evlilik teklif eden çiftler, enteresan kazalar, mobese kameralarına takılan ilginç görüntüler vs.**" şeklinde gösterilmekte, asıl çalışma amacı gizlenerek ve normalleştirilerek anlatılmaktadır. Öte yandan, bahsedilen ihbarlar bir sivil muhbirlik olup, ayrıca yasal bir dayanağı olmadan, farklı veya karşıt görüşlerde olanları devletin fişleyemediği noktada fişlenmesine yardımcı olmaktır.

İlk olarak, elinde kameralı cep telefonu olan herkesin trafik casusluğu yapmasını (*kurallara uymayan sürücüler için bile*) kabul edilemez buluyorum. Trafikteki kural ihlallerinin çözümü "**ihbar**" sisteminden geçmemektir. Ayrıca, bununla fişleminin ilerleyen süreç içerisinde daha normal bir algı yaratacağına inanmaktayım. Bunu şundan dolayı söylüyorum; ilk iki ihbar isteğinde neyin suç olduğu bir kışı tarafından belirlenirken bu sefer de yasalara aykırı durumlar bahane edilerek bir ihbar sistemi kurulmaktadır. Çünkü, hem tencere-tava hem de kızlı-erkekli ihbarların toplumun belirli bir kesimi tarafından (*iktidar gibi düşünmeyenler diyelim ya da siz ne derseniz*) "**fişleme**" olarak algılanmasına rağmen "**kurallara, trafiğe vs. yardımcı olmak**" adıyla fotoğraf çekilmesinin ve bununla ihbarda bulunulması gözden kaçırılmaktadır. Tıpkı Mobese haberleri ile yaratılmaya çalışılan algı gibi bu tarz ihbarların da asıl resmin üzerini örttüğünü düşünüyorum. Bu resim de fişlemenin ve devletin fişleme mekanizmasına yardımcı (*gönüllü, sivil muhbirlik*) olmanın ta kendisidir.

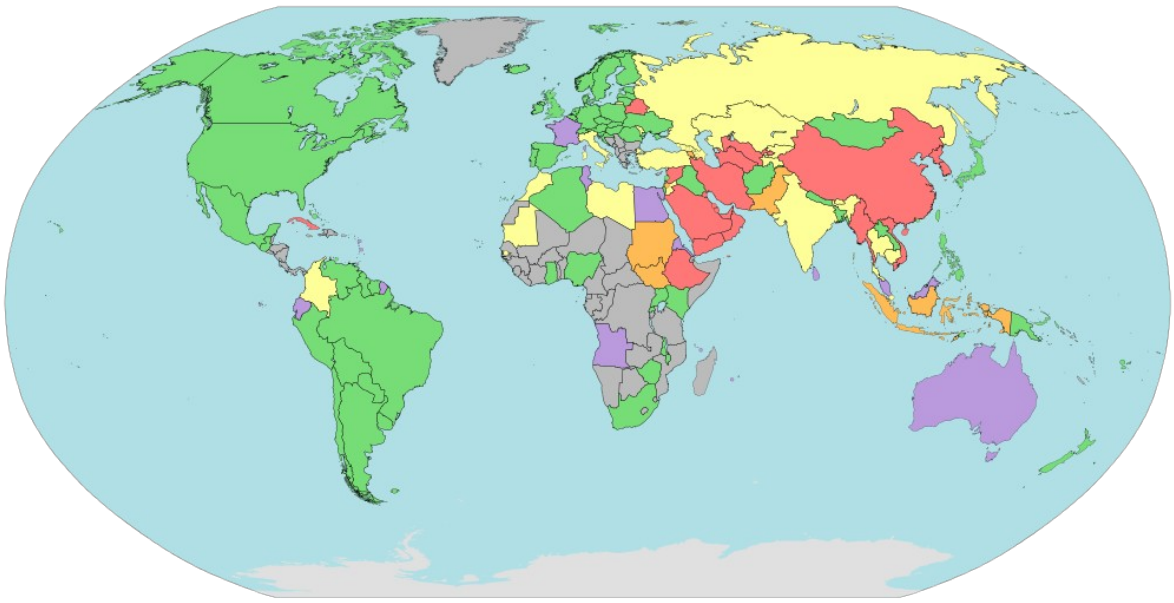
Son olarak, iktidar söz vermesine rağmen[16] fişlemeyi son vermemektedir. Askine, fişlemeyi normalleştirmekte ve bunun için de elinden geleni yapmaktadır. Fişlemenin zeminini hazırlayan ve normalleştiren bu tarz haberler ve ihbarların altında yatanlar iyi görülmelidir. Bugün için makul gelebilecek bir ihbar/ihbarlar ilerleyen süreçte fişleyen bir toplum mekanizmasına dönüşebilir/dönüştürebilir.

16 http://www.sabah.com.tr/Gundem/2010/09/11/sen_bildigini_oku_millet_de_okuyacak

4. Yeni 5651 ve Sansürün İşleyişi

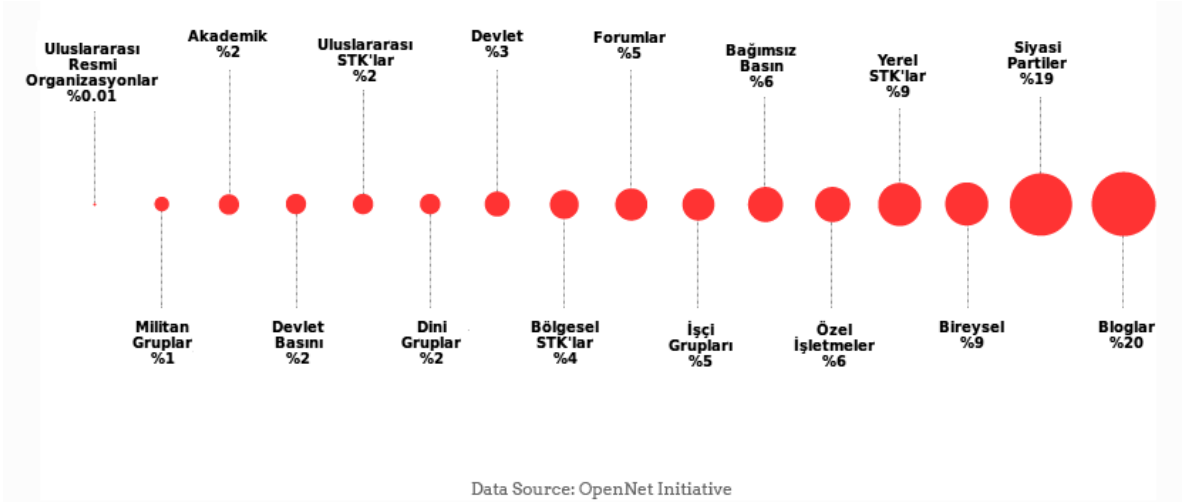
5651 yumuşatılarak geçmişken Internet sansürünün Türkiye'deki yumuşak yerine bir bakalım.

5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun sözde yumuşatılarak[17] meclisten geçti. Bizleri ilerleyen süreçte neler bekliyor, Türkiye'nin sansür konusunda dünyadaki yeri nedir, 5651 sayılı kanun sonrası ne olur, dünyada sansürlenen içeriklerin dağılımı ve bizdeki yansımaları ne olur tüm bunları merak etmekteyiz. İlk olarak, Türkiye'nin dünya Internet sansürü haritasında nerede yer aldığına bir bakalım.



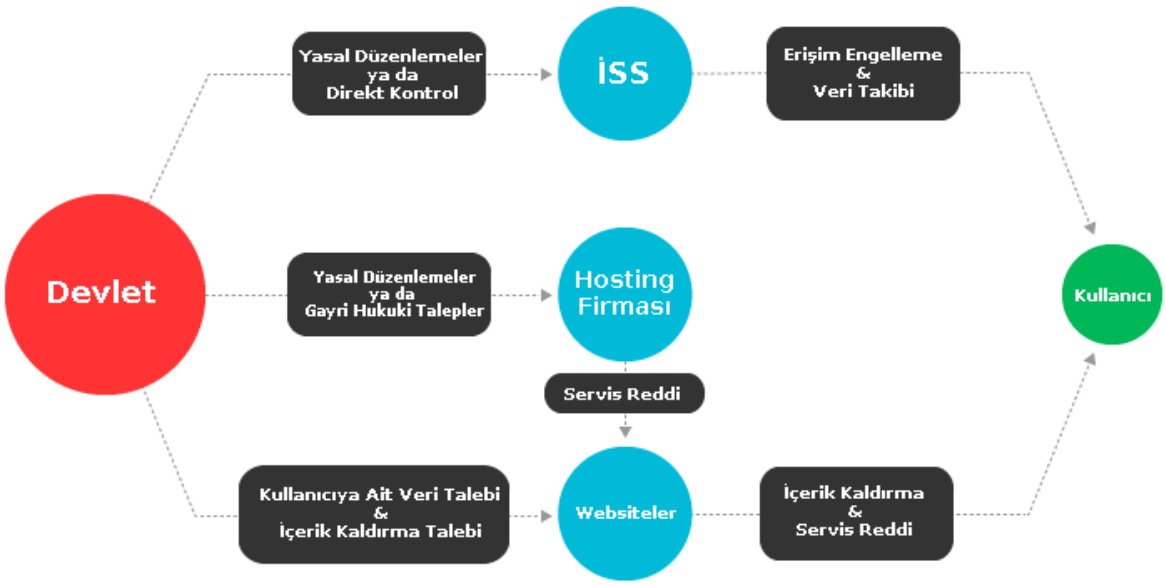
17 http://www.hurriyet.com.tr/teknoloji/25574246.asp

Yukarıda gördüğünüz harita 2013 yılı dünya sansür haritasıdır. Haritanın kaynağı için buraya[18] bakabilirsiniz. Ek olarak, diğer haritalar yerine renkleri için bu haritayı seçtim. Renklerin ifade ettiklerine gelirsek; radikal, oldukça, seçici, gözetim altında, düşük (*ya da yok*) ve veri yok şeklindedir. Haritaya Türkiye'de seçici bir sansür olduğu işlenmiştir. Bununla ilgili de hatırlarsanız çeşitli kelimelerin (*haydar, mini etek, liseli vs.*) filtrelendiği ve bunun üzerinden de sitelere erişimin yasaklandığını, TİB'in ise 2014 yılı itibariyle (*muhtemelen bahsettikleri sistemin otomatik olarak engellediği siteler*) 35702 siteyi, Türkiye'de ise toplamda 40124 sitenin engellediğini biliyoruz[19]. Fakat, 5651 sayılı kanun ile muhtemelen 2014 yılında Türkiye'de sansür oldukça veya radikal olarak renklendirilebilir bir hale gelebilir.



18 https://commons.wikimedia.org/wiki/File_talk:Internet_Censorship_World_Map.svg
19 http://engelliweb.com/kategoriler/

İkinci olarak, bizleri ilgilendiren diğer bir nokta dünyada sansürlenen içeriklerin ne olduğudur. Bu konundaki yüzdesel dağılım (*birincil kaynak: opennet initiative*[20]) yukarıda görüldüğü gibidir[21]. Yoğunluğun bloglar ve siyasi partilerde olması -*bence*- çok önemli bir noktadır. Özellikle 5651 sayılı kanun ile Türkiye açısından değerlendirdiğimizde, ilerleyen süreçte muhalefet partilerine ve bloglara, ardından bağımsız basına doğru çok ciddi bir sansür dalgasının yayılabileceğini (*bu kısmı benim öngörüm olarak alırsanız memnun olurum*) söyleyebiliriz.



Yeni 5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele

20 https://opennet.net/
21 http://archive.evanyou.me/censorship/

Edilmesi Hakkında Kanun'un[22] içeriğini yukarıdaki sansür işleyişi şeması üzerinden anlatalım. Devlet, yasal düzenlemelerin yanında İSS'larını direkt olarak kontrol edebilmek için tüzüğünü kendi onayladığı Erişim Sağlayıcıları Birliği adında bir birliğe üye olmaya zorlamaktadır. Bununla birlikte, bu birliğe üye olmayan servis sağlayıcıların faaliyette bulunamayacaklarını da ayrıca belirtmektedir. Böylece, erişim engelleri ve veri takibi (*phorm*[23]*, dpi*[24] *vs.*) taleplerinin bu birliğe yapılacağı, bunun bir sonucu olarak da taleplerin İSS'lere de yapılmış varsayılacağı söylenmektedir. Kısaca devlet, Erişim Sağlayıcıları Birliği ile İSS'leri direkt olarak kontrol edebileceği bir yapıya kavuşturmaktadır.

Ayrıca, yapılan erişim engelleri ve veri takibi için yasal bir koruma kalkanı da mevcuttur. Bu koruma kalkanına göre; "TİB Başkanlığı personelinin, yaptıkları görevin niteliğinden doğan veya görevin yerine getirilmesi sırasında işledikleri iddia olunan suçlardan dolayı haklarında ceza soruşturması açılmasına TİB Başkanı için ilgili Ulaştırma Denizcilik ve Haberleşme Bakanı, diğer personel için ise Bilgi Teknolojileri ve İletişim Kurumu Başkanı'nın izni aranacak." Bunu yukarıdaki veri takibi araçları ile ilişkilendirirsek sonucun ne kadar vahim bir boyutta olduğu çok net görebiliriz. Yani devlet, veri takibi için İSS'leri kontrol altında tuttuğu bir yapı içinde olmaya ve bu takipler sonucu doğabilecek suçların soruşturulması için de kendinden izin almaya zorluyor. Kısaca, beni bana şikayet edin demektedir.

22 http://www2.tbmm.gov.tr/d24/2/2-1928.pdf
23 http://enphormasyon.org/
24 http://www.enphormasyon.org/detay.html

Bir diğer nokta, yer sağlayıcıların (*hosting firmaları*) yasal düzenleme ile trafik kayıtlarını saklama süresi en az 6 ay en fazla 2 yıl olacak şekildedir. 5651 sayılı kanun TİB (*MİT kökenli Ahmet Çelik*) başkanına sansür için doğrudan yetki vererek -sözde- kanuna aykırı (*örneğin, kişilik hakları bahanesi ile*) fakat herhangi bir içeriğe erişim 4 saat içinde engellenebilecek (*24 saat içinde mahke karar verecek*) ve yer sağlayıcı kendisine bildirilen içeriği derhal çıkartmak zorunda kalacaktır. Gayri hukuki talepler ise tam bu noktada devreye girmektedir. Kendisiyle ilgili yapılan eleştiriden memnun olmayan bir "**bakan**" içerik hukuka uygun olsa bile (*örneğin, özel hayatı bahane ederek*) erişimi engelleyebilme yolu açılmış olacaktır[25]. Burada sadece bakanla sınırlamamak gerekir. İktidar, kendisini eleştiren tüm içeriklere ve bu içeriklerin birçoğu hukuka uygun olsa bile (*örneğin, özel hayatı tekrar bahane ederek*), erişime engelleyebilecektir. Diğer yandan, kayıt bilgilerinin nerede tutulduğu bu noktada çok önemli değildir. Kayıtların uzun süre tutulması ve istendiği takdirde (*hukuka uygun olsa bile*) devlete verilecek olması asıl problemdir. Fakat, Ulaştırma Bakanı Lütfi Elvan, "**kayıtlar devlette tutulmayacak**" diyerek[26] insanları yanlış yönlendirmektedir. Kendisine tabi yaptığı sağlayıcılar, istendiği takdirde tüm kayıtları vermek mecburiyetindedir.

Devlet, içerik kaldırma ve kullanıcıya ait veri taleplerini içerik sağlayıcılarından istemekteydi. Fakat, bununla ilgili olarak her zaman istediği sonucu alamamakta bazen de reddedilmekteydi[27]. Artık, içerik kaldırma ya da veri talebi ile uğraşmak yerine IP ve URL bazlı

25 http://www.bianet.org/bianet/bilisim/152663-bakana-internet-sitesi-engelleme-yetkisi
26 https://t24.com.tr/haber/ulastirma-bakani-internet-duzenlemesiyle-uygun-gorulmeyen-sayfalar-engellenecek/248493
27 http://www.bianet.org/bianet/ifade-ozgurlugu/148894-twitter-turkiye-ye-hic-olumlu-yanit-vermedi

engelleme getirerek, kuracağı birlik üzerinden İSS'lerin hizmetlere erişimi engellemesini sağlayacaktır. Bu şu demek oluyor; örneğin, Twitter'ın (*https://twitter.com*) tamamen erişime engellenmesi yerine Twitter kullanıcılarından herhangi birinin (*https://twitter.com/songuncelleme*) içeriğinin erişime engellenmesi veya tamamen erişime engellenen bir sitenin DNS (*VPN veya proxy hariç*) değiştirilse bile erişilememesidir. Böylece, devlet yapmış olduğu erişim engeli ya da veri isteği taleplerinde reddedilse bile içeriğe ya da tamamen yer sağlayıcıya erişimi engelleyebilecektir.

Yukarıda anlattıklarımı en basit şekliyle bir kolunu şemaya uygun olarak kısaca tekrar anlatayım. Devlet, yasal bir düzenleme ile İSS'leri oluşturacağı birliğe üye yapmaya mecbur ederek İSS'lerin direkt kontrolünü sağlar. Böylece veri takibi ve erişim engelini de kendine yani tekele yükler. Bu da içeriğin kaldırılmasından engellenmesine, veri takibinden kullanıcının Internetteki hareketlerinin izlenmesine kadar çok geniş çaplı bir alanı kapsar. Tüm bunları toparlayacak olursam, devlet kendi denetiminde ve üyeliği zorunlu tuttuğu bir birlik kurarak Internet'te veri takibi ve erişim engelinin gayri hukuki yolunu açmış, ayrıca bunu yasal bir düzenleme ile yapmıştır. Bununla birlikte, Türkiye'de zaten radikal bir sansür mevcuttur. Bu konuda bir örnek (*çoğaltılabilir elbette*) göstermem gerekirse, hiç düşünmeden Guillaume Apollinaire Davası[28] diyebilirim. 5651 sayılı kanun ile oluşturulacak yeni birlik ve işleyiş de Internette "**seçici**" olan sansürü "**radikal**" sansüre çevirecektir.

28 http://www.bianet.org/bianet/ifade-ozgurlugu/151660-guillaume-apollinaire-davasi-ifade-ozgurlugune-aykiri

Şimdi soruyorum, sizce sansür haritasında 2014 yılı sonu için Türkiye'nin yeni rengi (*benim ifademi bunun dışında tutarak*) ne olacaktır?

Ekleme (17.01.2014): Bugün t24'te 'Emniyet ve yargıdaki görevden almaların merkez üssü TİB'[29] başlıklı bir haber yayımlandı. Haberde TİB'e MİT kökenli Ahmet Çelik'in atanmasından sonra cemaate yakın kamu görevlilerinin listelerine yönelik çalışma başlatıldığı ve teknik takiplerin TİB'in "**ana dinleme sistemi**" aracılığı ile kontrol edildiği söyleniyor. Yazıyla tamamen tutarlı olması açısından önemli bir haberdir.

Ekleme (17.01.2014): Yeni bir haber daha. 'Dinlemenin merkezi' TİB'de tüm daire başkanları görevden alındı[30] başklı bu haberde de 5 TİB daire başkanın görevden alındığı ve yerlerine MİT kökenli isimlerin geleceği söylenmiş. Türkiye'yi artık radikal olarak boyayabiliriz.

Ekleme (24.01.2014): Vimeo erişime engellendi[31].

Ekleme (24.01.2014): Soundcloud erişime engellendi[32].

Ekleme (27.01.2014): Vagus.tv erişime engelledi[33]. (*Özgür basın*)

---

29 http://t24.com.tr/haber/emniyet-ve-yargitaydaki-gorevden-almalarin-merkez-ussu-tib/248562
30 http://t24.com.tr/haber/dinlemenin-merkezi-tibde-tum-daire-baskanlari-gorevden-alindi/248620
31 http://elmaaltshift.com/2014/01/09/vimeo/
32 http://birgun.net/haber/soundclouda-sumeyye-engeli-10405.html
33 http://www.bthaber.com/simdi-de-vagus-tv/

Ekleme (31.01.2014): Bilgi Teknolojileri İletişim Kurumu ile Telekomünikasyon İletişim Başkanlığı, T24'e CHP'nin soru önergesi haberini[34] yayından kaldırması için tebligat yolladı. Haberin ayrıntıları burada[35]. Özgür basın demiştim değil mi? Buna dolaylı yoldan siyasi partiye ait haber ve içeriği de ekleyebiliriz.

34 http://t24.com.tr/haber/chpli-orandan-erdogana-sabah-ve-atv-icin-satin-alma-talimati-verdiniz-mi/247740
35 http://t24.com.tr/haber/btk-ve-tibden-t24e-chpnin-soru-onergesi-icin-yayini-durdur-yazisi/249930

5. Sansürün Bizi Etkileme Derecesi

> Aklımdan geçenleri tam olarak ifade edebildiğimden emin değilim. Yazı da gece sansür konusunda artık farklı şeyler söylemekten bahsederken birkaç cümleden çıktı, buraya kadar geldi. Umarım okurken keyif alır (*ne keyfi, dikkatinizi çeker diyelim*) ve görüşlerinizi belirtirsiniz.

5651 sayılı kanun ile gelecek Internette sansür ve etkileri tartışıladursun, ben biraz daha konuyu farklı bir noktaya çekip bir eleştiri getireceğim. Bunun nedeni ise bakış açısını biraz daha farklılaştırabilmek ve daha farklı düşünebilmektir. Öncelikle, sansürün kelime anlamına (*TDK*[36]) bir bakalım:

Her türlü yayının, sinema ve tiyatro eserinin hükûmetçe önceden denetlenmesi işi, sıkı denetim.

Bizler de tanım olarak farklı bir şey beklemiyorduk. Bizleri en çok ilgilendiren kısım ve yazının temel noktasını oluşturacak şey de "**hükümet-ler-ce önceden denetlenmesi işi**". Bildiğimiz üzere, hükümetleri oluşturan partiler ve her partinin de kendine has bir yoğurt yiyişi vardır. Denetim de tam bu noktada önem kazanır çünkü partiler kendi ideolojilerini ön planda tutarak bir denetim süzgeci oluşturacaktır. Fakat, bu süzgeç ne kadar farklı olursa olsun, sansür bir korkuluk gibi durmaya ve baki kalmaya devam etmektedir. Bununla birlikte, sadece sansürlenen "**şeyler (içerikler)**" değişen hükümetlere göre farklılık göstermektedir.

---

36 http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52e1d64c272cf7.42316638

Sansürün değişen hükümetlere göre gösterdiği farklılığı şöyle anlatayım; daha "**muhafazakar**" bir partinin iktidarlığında bir kitap "**müstehcen**" bulunurak sansürlenebiliyor (*veya böyle bir girişimde bulunulabiliyor*), televizyon yayınlarında çok çeşitli sansürler (*böyle dekolte olmaz*[37]) görülebiliyor, Internet üzerinde çeşitli kelime grupları bu muhafazakarlık çerçevesinde (*örneğin ateizm*[38]) filtrelenerek sansürlenebiliyor. Öte yandan, darbelerde sıkça yapılmış sansürleri (*kitaptan şarkıya, çok geniş alanda*) görebiliyoruz veya başka bir parti iktidar olduğunda Türkiye'de yaşayan farklı etnik gruplara, bu etnik grupların dillerine, yayınlarına veya haberlere sansür uygulanabiliyor. Bu durumla ilgili birçok örnek senaryo oluşturulabilir. Benim dikkati çekeceğim nokta bu sansürlerin bizleri nasıl, ne yönde etkilediği, bizleri etkileme derecesi ve neden baki kaldığıdır.

Konuyla ilgili olarak Apollinaire davasını[39] ele alalım. Kitap mevcut iktidar tarafından müstehcen ve muahfazakar yapısına ters bulunduğu için sansürlenmek istenmektedir. Bu sansürün bizleri nasıl etkilediğine gelince; edebiyatla hiç ilişkisi olmayan bir birey bu sansürden olumsuz yönde etkilense de onun bu sansürden etkilenme derecesi edebiyatla ilişkili bir bireye kıyasla daha düşüktür. Edebiyatla ilişkili bir başka birey de hem olumsuz hem de daha yüksek derecede etkilenmektedir. Bu noktada ön plana çıkan şey -yani etkileme derecesinin önemi-, birey bir sansürden ne kadar az etkilenme derecesine sahipse o sansürü görmezden gelebilme derecesi de aynı oranda artmaktadır. Çünkü, edebiyatla ilişkisi olmayan bu birey, ilgili alanına girmediği için bu kitabın sansürlenmesiyle ilgilenmemekte veya

37 http://vagus.tv/2013/10/07/huseyin-celiki-isyan-ettiren-dekolte/
38 http://bilimvedin.net/bilimvedin/din-ve-yasam/ateizme-internet-sansuru/
39 http://www.haberler.com/apollinaire-nin-mustehcen-kitap-davasi-5435871-haberi/

konuya ilişkin bilgi sahibi olsa da görmezden gelmektedir.

Bir başka ve görülmesi daha net bir örneğe gelecek olursak, Türkiye birçok etnik grubun diline sansür uygulayan iktidar-lar vardır/olmuştur. Bu etnik gruba üye bireyler kendi dillerine uygulanan bu sansürden olumsuz yönde ve yüksek derecede etkilenirken, bu etnik gruba üye olmayan, bu dili konuşmayan bireyler ise düşük -*hatta yok sayılacak*- düzeyde etkilenmektedirler. Ayrıca, etkilenmediği için bu konuda yapılan bir sansürün ne tür boyutlarda yıkım oluşturduğunu da bilememektedir. Sansüre uğrayan etnik grup sayıca ne kadar az olursa (*sayıca çok olması da görüldüğü kadarıyla görmezden gelinmeye engel olmuyor*) ve görmezden gelen veya ilgilenmeyen (hatta destekleyen) kesim ne kadar kalabalık olursa sansür o kadar çok normalleştirilmekte, kalabalık kesim (*çoğunluk*) tarafından meşru bir şeymiş kabul edilmekte, bu etnik grup (*azınlık*) üzerinde böyle bir algı oluşturulmaya çalışılmaktadır.

Son bir örnek de kendimden vereyim. Benim için dini bir kitabın veya dini bir Internet sitesinin sansürlenmesi çok bir şey ifade etmiyor ve benim bundan etkilenme derecem yok denecek kadar azdır. Fakat, ben bu sansür karşısında tepki göstermezsem veya görmezlikten gelirsem bu yaptığım yapılan sansürü ve ileride yapılacak sansürleri meşru kılacak bir zemin hazırlar. Ayrıca inancım, görüşüm, dilim ne olursa olsun asla kabul edilebilir bir davranış değildir. Eğer bir duruş arıyorsanız, buna empati yapabilmek diyebilirsiniz.

Yukarıda gösterdiğim örnekleri dikkate alarak sansürün baki kalmaya devam etmesinin en büyük katalizörlerinden biri -bence- sansürün bizleri etkileme derecesidir. Bizler bir sansürden ne kadar az etkileniyorsak, o konuda o kadar çok görmezden gelebiliyor, ilgilenmeyebiliyor, normalleştirebiliyor veya bana dokunmayan yılan diyerek geçiştirebiliyoruz. İşte tam da bu noktada hataların en büyüklerinden birini gerçekleştiriyoruz. Sansür her ne olursa olsun sansürdür ve kime veya neye yapılırsa yapılsın, bizleri ne kadar az etkilerse etkilesin (*veya hiç etkilemesin*) bunun karşısında olmak gerekir.

Sonuç olarak, beni/bizi ilgilendirmiyor, beni/bizi etkilemiyor diyerek sansürü ne kadar çok görmezden gelirsek o kadar çok normalleştirir ve meşrulaştırır, bir önceki hükümette bizi etkilemeyen -veya çok az etkileyen- bir sansür bir sonraki hükümette farklı bir formda ve bizleri daha yüksek düzeyde etkileyebilir. Ayrıca, sansüre karşı çıkmak azınlığın veya belirli kitlelerin, etnik grupların veya belirli bir konuda ortak görüş sağlamış çoğunluğun değil, herkesin yararınadır. Malesef her türlü sansüre (*etkilensin veya etkilenmesin*) her zaman tepki gösteren küçük bir kesim var ve artık bunun olabildiğince büyümesi gereklidir. Çok şey istediğimin farkındayım ama sansür konusunda -*ve birçok konuda*- zihniyetin değişmesi gereklidir. Değişmediği sürece sansür mücadelesi bir daire etrafında aynı şeyleri tekrarlayan ve farklı yönlere koşma mücadelesinden öteye geçemeyecektir.

Not: Gelen bir e-posta üzerine sıkça yapılan bir mantık hatasından bahsetmem gerekli oldu.

A- Sansür olmamalı.

B- Hayır efendim, örneğin çocuk pornosu serbest olur ve önünü alamayız. Bu asla istemeyeceğimiz bir durumdur ve herkes olumsuz etkilenir.

Buna korkuluk mantık hatası denilmektedir. A ifadesinde çocuk pornosunun gibi aşağılık bir şeyin serbest olmasından bahsetmezken B bir korkuluk yaratarak (*çocuk pornosu*) tartışmayı savunulması zor bir tarafa çekmektedir. Kaldı ki çocuk pornosu (*pedofili*) ile mücadele için sansür araçlardan biridir. Tek başına sansür bir anlam ifade etmez.

6. Youtogg

Kendi işlerimi kolaylaştırmak için bir script (*betik*) yazdım. Bunu da sizlerle paylaşmadan olmazdı. Genelde saçma isimler bulmakta üzerime yoktur. Bu betik için de aynısı oldu diyebilirim.

Ne işe yarıyor?

Youtogg, hemen hemen birçok video sitesinden (*Youtube, Vimeo, Dailymotion vd.*) video indirip bunları ses formatına (**.ogg*) dönüştürmenize olanak sağlayan basit bir betiktir. Bunun dışında, Tor ağı üzerinden indirme seçeneği hariç hiçbir özelliği yoktur.

Nasıl çalışıyor?

İlk olarak, kullanıcı dizini altında "**youtogg**" dizini oluşturuyor. İndirdiği videolar ve dönüştürdüğü ses dosyalarına buradan erişebileceksiniz. Ardından, indirmek istediğiniz video linkini girerek istediğiniz formatı (*mp4, flv, webwm vd.*) ve çözünürlüğü seçeceğiniz bir ekran çıkmaktadır. Burada 18, 22, 143 vd. gibi seçimler yapıyorsunuz. Bu noktada bağlantı hızınıza göre hareket edebilirsiniz. Bununla birlikte, video indikten sonra sizlere dönüştürülecek çıktının adını sormaktadır. Örneğin, burada şarkının ve sanatçının adını veya ikisini birden (*ya da ne yazarsanız*) yazabilirsiniz.

Kurmanız gereken birkaç uygulama/kütüphane var. Bunlar, youtube-dl, ffmpeg ve libvorbis. Dağıtımınızın paket yöneticisinden aratarak kurabilirsiniz. Tor ağı seçeneği opsiyoneldir. Eğer, Tor ağı üzerinden indirmek isterseniz tor ve polipo paketlerini de kurmanız,

polipo'yu tor için ayarlamanız gerekmektedir. Kısaca bir polipo ayarı (*/etc/polipo/config*) göstermem gerekirse:

```
daemonise=false
diskCacheRoot=/var/cache/polipo/
proxyAddress=127.0.0.1
proxyName=localhost
serverSlots=4
serverMaxSlots=8
cacheIsShared=true
allowedClients=127.0.0.1
socksParentProxy = localhost:9050
socksProxyType = socks5
```

Neden?

Öncelikle, bu betik benim için gerekli. Flash ve HTML5 kullanmıyorum. Genelde bir video izleyeceksem bunu youtube-dl ve mplayer ile birlikte yapmaktayım. Fakat, dinlediğim şarkıları telefonda veya mp3 çalarda da bulunmaları ve tekrar tekrar indirmemek için böyle bir şey yaptım. Benim işimi fazlasıyla görüyor. Diğer yandan, belki ilgisini çeken birileri betiği geliştirmek isteyebilirler. Ek olarak, bir yazılımcı değilim. Kod yazmayı bilmiyorum.

Kod

```
#!/bin/bash
#
# Youtogg is a basic video to ogg conversion script.
#
# Dependencies: youtube-dl, ffmpeg, libvorbis
# Optional: tor, polipo
# Contact: kusburnu@riseup.net
###
# Welcome screen
_welcome () {
        echo $@ | sed -e 's/^/../' -e 's/$/../' -e 's/./*/g'
        echo $@ | sed -e 's/^/* /' -e 's/$/ */'
        echo $@ | sed -e 's/^/../' -e 's/$/../' -e 's/./*/g'
        }
_welcome "WELCOME TO YOUTOGG"
echo
###
# Folder check
_folder_check () {
        if [ -d ~/youtogg ]
        then
                read -p "Video Link: " video
                echo
        else
              echo "Creating youtogg folder"
                mkdir ~/youtogg
                read -p "Video Link: " video
                echo
        fi
}
```

```
_folder_check "$@"
###
# Video download
_video_download () {
        while true
        do
                echo
                read -p "Do you want to torify? (Y/N) " answer1
                echo
                case $answer1 in
                        [yY]* ) cd ~/youtogg && filename=source &&
                                youtube-dl -F --proxy "127.0.0.1:8123" $video &&
                                echo && read -p "Choose your video format: " format &&
                                echo && youtube-dl -f $format -o $filename --proxy "127.0.0.1:8123"  $video
                                break;;

                        [nN]* ) cd ~/youtogg && filename=source &&
                                youtube-dl -F $video && echo && read -p "Choose your video format: " format &&
                                echo && youtube-dl -f $format -o $filename $video
                                break;;

                * )     echo "Y or N, please!";;
        esac
done
}
_video_download "$@"
###
# Name for the output file
_filename () {
        echo
```

```
        read -p "Output filename: " name
        echo
}
_filename "$@"
###
# Converting video to ogg
_convert () {
                while true
                do
                        ffmpeg -i $filename -vn -acodec libvorbis "$name.ogg"
                        echo
                        read -p "Do you want to keep video file? (Y/N) " answer2
                        echo
                        case $answer2 in
                                [yY]* ) mv $filename $filename.$(date +%m%d%Y_%H%M
%S)
                                        break;;

                                [nN]* ) rm $filename
                                        break;;

                * )     echo "Y or N, please!";;
        esac
done
}
_convert "$@"
###
# Log
_log () {
        echo "$video = $name.ogg" > youtogg.log.$(date +%m%d%Y_%H%M%S)
}
_log "$@"
```

```
###
# Loop
_loop () {
        while true
        do
                echo
                read -p "Do you want to convert again? (Y/N) " answer3
                echo
                case $answer3 in
                        [yY]*  ) _folder_check "$@" && _video_download "$@" && _filename "$@" && _convert "$@" && _log "$@"
                                break;;

                        [nN]* ) echo "Goodbye!"
                                exit;;

                * )     echo "Y or N, please!";;
        esac
done
}
_loop "$@"
```

Son olarak...

Bu kodu aynen bir metin düzenleyicisine kopyalayıp kaydedin. **chmod +x dosyadı** ile çalıştırılabilir hale getirin. Son olarak, terminalden çalıştırın. Hepsi bu kadar. Kullanır ve yorum yaparsanız memnun olurum. Önerilerinizi ve geliştirmelerinizi de eklerseniz mükemmel olur.

7. Sansürde Son Gelişmeler

> Hukuka aykırı kanun tasarısı, insan haklarına aykırı kurum TİB. Ne derseniz diyin. Bunun adı açık ve net biz imza attığımız insan hakları sözleşmesini tanımıyoruz demektir.

Yeni 5651 sayılı "**İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayın Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**" tasarısı torba yasa içine konularak mecliste görüşmelerine başlandı. Fakat, gelen tepkilerden sonra oturum 4 Şubat tarihine ertelendi. Tasarının TİB'e sağladığı koruma kalkanı[40] ve MİT kökenli başkanların atanması[41] ile yerli NSA yapısına dönüşeceği defalarca belirtildi, yazıldı ve çizildi. Bununla birlikte, torba yasayla 5651 sayılı kanun henüz geçmemesine rağmen TİB hukuka aykırı olarak erişim engelleme ve içerik kaldırma taleplerinde bulunmaya başladı bile. Sırayla erişime engellenen siteleri ve gerekçelerine bir bakalım:

Vimeo

Vimeo, 8 Ocak 2014 tarihinde "**müstehcenlik**" gerekçesi ile erişme engellendi[42]. Erişime engellenme asıl nedeni Başbakan'ın kardeşi Mustafa Erdoğan'a ait bir videonun sitede yer almasıydı. Video, özel hayatın gizliliğini ihlal etmektedir. Fakat, bunun için Vimeo ile iletişime geçmek yerine siteye erişimin tamamen engellenmesi tercih edildi. İçerik silindikten ve Vimeo bir süre erişime engellendikten sonra karar kaldırıldı.

---

40 https://t24.com.tr/haber/internet-yayinciligina-agir-denetim-ve-yaptirimlar-geliyor/247549
41 http://t24.com.tr/haber/dinlemenin-merkezi-tibde-tum-daire-baskanlari-gorevden-alindi/248620
42 http://engelliweb.com/url/vimeo-com

Soundcloud

Soundcloud, 16 Ocak 2014 tarihinde Sümeyye Erdoğan'ın telefon görüşmelerine ait ses kaydının yayımlanmasından sonra erişime engellendi[43]. Bununla birlikte, yayımlanan ses kayıtlarında sadece Sümeyye Erdoğan yoktu. Ayrıca, Başbakan'a ait ses kayıtlarını da içermekteydi. Aynı Vimeo'da olduğu gibi içeriğin kaldırıması talebi yerine site tamamen erişime engellendi ve Soundcloud şu an hala engelli durumdadır.

Vagus.tv

Vagus.tv, 16 Ocak 2014 tarihinde "**koruma tedbiri**" kararı ile habersizce erişime engellendi[44]. Habersizceden kasıt, Vagus.tv'ye herhangi bir bildirimde bulunulmadan direkt olarak engellenmesidir. Ayrıca Vagus.tv sahibi Serdar Akinan, engelleme ile ilgili bilgi almak için TİB'e giden avukatlarının hiçbir yetkileye ulaşamadıklarını ve Cumhuriyet Başsavcısı'nında böyle bir kararının olmadığını belirtti. Karar olmadığı halde TİB'in hukuka aykırı bu engeli bir yana, henüz kanun tasarısı kabul edilmeden yapmış olduğu engel için cevap vermeye tenezzül bile etmemesi ilerleyen süreçte özgür basına yapılacakların bir habercisidir. Ek olarak, hala erişime engellidir.

T24 ve soL Haber Portalı

T24[45] ve soL Haber Portalı[46], 1 Şubat 2014 tarihinde BTK ve TİB tarafından yayımlamış oldukları "**CHP'li Oran'dan Erdoğan'a: Sabah ve ATV için satın alma talimatı verdiniz mi?**"[47], "**Sabah-ATV**

43 http://engelliweb.com/url/soundcloud-com
44 http://engelliweb.com/url/vagus-tv
45 http://t24.com.tr/haber/btk-ve-tibden-t24e-chpnin-soru-onergesi-icin-yayini-durdur-yazisi/249930
46 http://haber.sol.org.tr/medya/tib-ve-btkdan-sola-bu-haberi-kaldir-mesaji-haberi-86979
47 http://t24.com.tr/haber/chpli-orandan-erdogana-sabah-ve-atv-icin-satin-alma-talimati-verdiniz-mi/247740

havuzunu Erdoğan mı doldurdu?”[48] ve “**2. dalgada adı geçen kişiler hakkındaki yakalama kararı kaldırıldı!**”[49] haberlerinin yayından kaldırılması için tebligatta bulunuldu. Bu tebligata göre; “**04/05/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**“‘a dayanarak konu içeriğin çıkarılması istenmektedir. İçeriklerin hukuka aykırı bir şey içermemelerine rağmen böyle bir istekte bulunulmuş, ayrıca kaldırılmadığı takdirde Türkiye’den erişime engelleneceği de bildirilmiştir. Burada sadece özgür basına uygulanan sansür bir yana bir siyasi partiyle ilgili habere ve içeriğe de dolaylı bir sansür söz konusudur.

Yukarında bahsedilen erişim engelleri ve içerik kaldırma talepleri TİB’in Internet üzerinde hüküm verebilen ve hükümetin sansür isteklerini yerine getiren bir kurum olduğunun tıpkı bugüne kadar yaşanan süreçte olduğu gibi açık bir delilidir. Diğer yandan, TİB’in MİT kökenli bir yönetime kavuşması, yeni 5651 sayılı kanun tasarısı ile de yasal bir koruma kalkanına sahip olması radikal sansürün en büyük habercisidir demiş ve özgür basından siyasi partilere doğru bir sansür dalgasının başlayacağını öngörmüştüm[50]. Bugün yaşananlara baktığımızda sansür işleyişinin bu ifademe tamamen uyduğunu gördüm.

Ek olarak, belirtmeden edemeyeceğim birkaç nokta var. “**Daha yeni 5651 sayılı kanun çıkmadan böyle oluyor**” dediğiniz anda

48 http://haber.sol.org.tr/medya/sabah-atv-havuzunu-erdogan-mi-doldurdu-haberi-86756
49 http://haber.sol.org.tr/devlet-ve-siyaset/2-dalgada-adi-gecen-kisiler-hakkindaki-yakalama-karari-kaldirildi-haberi-86059
50 https://network23.org/kame/2014/01/16/yeni-5651-ve-sansurun-isleyisi/

kanun çıktıktan sonra yapılacak sansürleri bir ister istemez kabul ettiğiniz veya kanunda yazıyor yapacak bir şey yok dediğiniz anlamına da geliyor. Elbette böyle bir şeyi kimse istemez fakat bunu da görebilmek önemlidir. Ayrıca, yeni tasarı insan haklarına aykırıdır. Aykırı bir kanunun kararları da doğal olarak hukuka aykırı olacaktır. Türkiye'nin de altına imza attığı Avrupa İnsan Hakları Sözleşmesi'ne aykırı bir kanun ile yapılacaklara "**hukuka uygundur**" demek abesle iştigaldir. Bir diğer nokta da, TİB hukuka aykırı hareket ederek 5651 sayılı kanun tasarını meşrulaştırmaya çalışmakta, yaptıkları ile kanun da desteğini alarak yeni bir yasal zemin hazırlamaktadır.

Malesef, bizleri radikal, fişlemeye dayanan, toptan gözetimci ve insan haklarına aykırı sansürlerlerin olacağı daha da kötü bir dönem beklemektedir. Yeni 5651 sayılı kanun daha çıkmadan TİB hukuka aykırı yaptırımlarda bulunarak MİT kökenli yeni yapısı ile yerli NSA olma yolunda hızlı adımlarla ilermekte, Internetin hükümet süzgeci olmaktadır. Internet güçle kutsanmış iktidarın mülkü, iktidarın bizlere dayattığı sansürcü anlayış da hukuk değildir.

8. Türkiye'nin Internetteki Yeni Yeri

> *Türkiye'nin Internetteki yeni yeri mağmadır. Yerin dibinin de dibidir. Buradan çıkartacak ve bizleri bu utançtan kurtaracak olan da ne muhalefet ne de iktidardır. Sadece bizleriz.*

Yeni 5651 sayılı kanun tasarısı 5 Şubat 2014 tarihi itibariyle mecliste oylanarak kabul edildi[51]. Bununla ilgili olarak meclisin bu yasanın görüşüldüğü andaki bir ekran görüntüsünü paylaşayım (*Şevket'e[52] çok teşekkürler)*:

51 http://yesilgazete.org/blog/2014/02/06/internet-yasagi-meclisten-gene-kurulunda-kabul-edildi/
52 https://twitter.com/sevketuy

Sizlerle paylaştığım bu ekran görüntüsü ile duygu sömürüsü falan yapmıyorum. Dikkat ettiyseniz kanun tasarı anlaşılmasın diyerek televizyonlara "**Aile ve Sosyal Politikalar Bakanlığı'nın Teşkilat ve Görevleri Hakkında KHK'da Değişiklik Yapan Kanun Tasarısı**" adı altında yansıtıldı. Diğer yandan, gördüğünüz boş koltuklar bir insan hakkı olan Internete, gizliliğinize, düşünce özgürlüğünüze, ifade özgürlüğünüze, inanç özgürlüğünüze, bilime, bilim etiğine, açık bilgi akışına, gelişime, ilerlemeye ve Internetten para kazananların ekmeğine (*ve sayamadığım daha birçok hak ve özgürlüklere*) yani iktidar destekçi olun veya olmayın sizlere ve geleceğinize vurulmuş en büyük darbedir.

Şimdi kısaca birkaç şeyi son bir kez daha netleştirelim. Sansür; her türlü yayının, sinema ve tiyatro eserinin hükûmetçe önceden denetlenmesi işi, sıkı denetim demektir. Bu, TDK'nin verdiği tanımdır[53]. Tabi ki ilerleyen süreçte bu da değiştirilmezse[54]. Devamlı ifade edilen ve ettiğim bir diğer şey de TİB'in başına MİT geçmişi olan Ahmet Çelik'in gelmesidir[55]. Sizlere MİT'in sitesinden bir alıntı yapayım (*umarım bu cezai takibata neden olmaz inşallah dinimiz amin maşallah*):

İstihbaratta gaye, doğru haber almak ve devleti bir süprizle karşı karşıya bırakmamaktır.

Bir de istihbaratın kelime anlamına bakalım. Herhangi bir Türkçe sözlüğü açıp baktığınızda kelimenin Arapça kökenli ve çoğul bir kelime olduğunu göreceksiniz. Anlamı ise "**haberler**" ve "**haber alma**"

53 http://tdk.gov.tr/
54 http://www.radikal.com.tr/turkiye/tdk_capulcu_tanimini_degistirdi_mi-1136483
55 http://t24.com.tr/haber/emniyet-ve-yargitaydaki-gorevden-almalarin-merkez-ussu-tib/248562

şeklinde yazmaktadır. Teknik olarak istihbarat ise imkanları ve araçları kullanarak bilgi temin etmek, bu bilgiyi işlemek, yorumlamak ve bundan bir sonuç çıkarma sürecini ifade eder. TİB yeni kanun ile bizlere ait bilgiyi (*veriyi*) temin etme, bu veriyi işleme, yorumlama ve bundan bir sonuç çıkarma (*fişleme*) sürecine yasal olarak sahip olmuştur. Ayrıca, bu gelenekten gelen bir ismi de kendini başkan yapmıştır.

Artık yeni kanun ile birlikte bunu şöyle yorumlayabiliriz: “**17 Aralık 2013 tarihinde başlayan ve devletleşen AKP, AKP’leşen devlet bir yolsuzluk operasyonu süpriziyle karşı karşıya kalmış, buna benzer bir durumla tekrar karşılaşmamak, engellemek ve bundan korunmak için TİB, MİT geçmişi olan Ahmet Çelik başkanlığı ve yeni kanun ile Internette her türlü veriyi önceden denetleyecek, temin edecek, işleyecek, yorumlayacak, bundan sonuç çıkartacak ve sıkı denetim yapacak, insan haklarına aykırı bir yapıya yasal olarak kavuşmuştur.**” Ayrıca, ülke tarihinin en büyük toptan gözetimci fişlemesi ile karşı karşıyayız. Bu yapı yüzünden sadece biz karşı çıkanlar kaybetmeyeceğiz. Herkes kaybedecek. Bunun ötesi berisi yoktur.

Sonucu bu sefer uzun uzun yazmayacağım. Okuyanlar artık az çok ileride neler olacağını, neler yaşayacağımızı biliyor. Bununla birlikte, yeni 5651 sayılı kanun tasarısı için yazılar yazdım ve sansürü elimden geldiğince burada anlattım. Bu yazılar kimilerine ulaştı, kimileri okuduğu halde görmezlikten gelmeye devam etti. Sansüre karşı empati yapın dedim fakat çok da ciddiye alınmadım. Hala da aynı konuda ısrar ediyorum, empati yapın. Empati yapmayı öğrenin. Bu toptan gözetimci,

fişlemeci sansür yasası, *-tekrar tekrar vurguluyorum-* ilgili ilgisiz herkese zarar verecektir. Bunun seni, beni, onları olmaz. Lütfen bunu görün. Son olarak, ümitsizliğe kapılmayın. Sansüre karşı verilen bu mücadele hiçbir zaman bitmeyecektir.

9. I2P'ye Giriş

> *Bir başka anonim ağ, I2P. Bir başka giriş yazısı, I2P'ye Giriş. Eksik olduğunu biliyorum. Fakat iş görmeyecek, anlaşılmayan noktaları gideremeyecek kadar kötü de değil.*

Yeni 5651 sayılı kanun tasarısı 5 Şubat 2014 tarihinde kabul edildi[56]. Ben de Tor'a Giriş[57] yazısı gibi bir I2P'ye Giriş yazısı hazırlamaktaydım. Fakat, hem gündemin yoğlunluğu hem de kendi yoğunluğum nedeniyle bunu hep arka plana atıyordum. Şimdi bunu acilen yayımlamak şart oldu. Teknik olarak yazı biraz eksik. İlerleyen süre içerisinde bunu gidereceğim. Öte yandan, yazı içerik olarak kafanızdaki soru işaretlerini giderecek düzeyde ve kullanım açısından pek bir eksik içermiyor. Yazıyı okurken ve I2P kullanırken şunu aklınızdan hiç çıkarmayın; "**I2P kullanan bir kişi gizli değildir. Gizli olan şey tıpkı router'ın (*yönlendirici*) bağlı olduğu belirli bir hedef gibi kullanıcının bu anonim ağda ne yaptığına dair bilgidir.**"

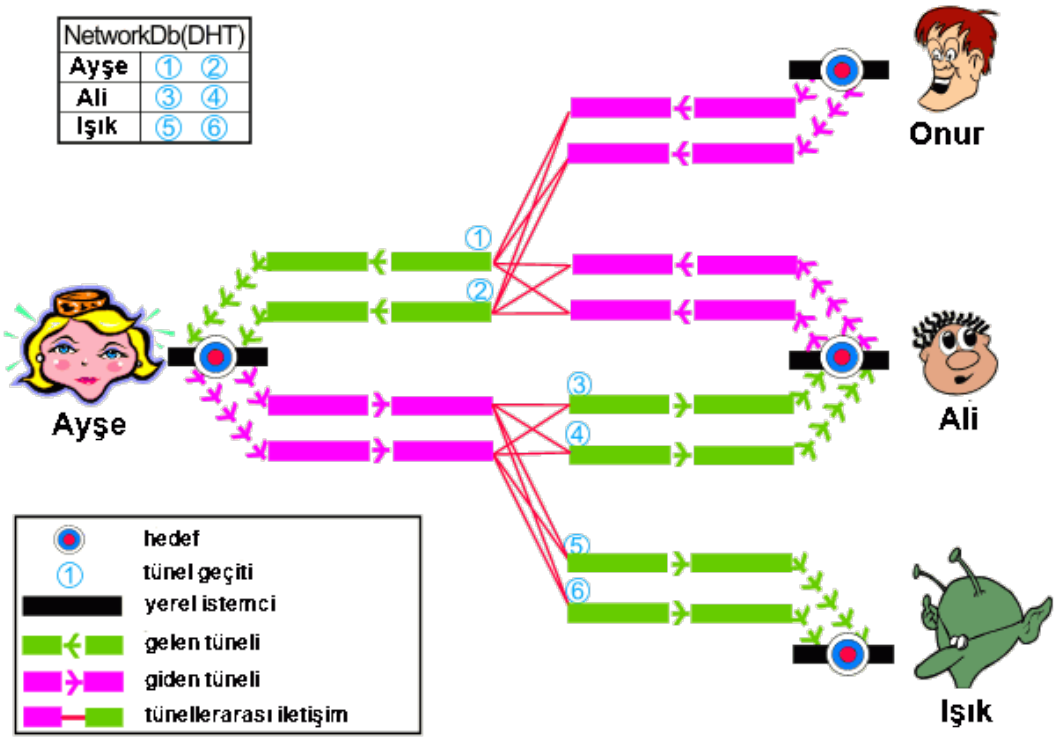
I2P[58]; açık kaynak, P2P anonim bir ağ olup, basit bir katman oluşturarak çeşitli araçların birbirleriyle güvenli bir iletişim kurmalarını sağlayan özgür bir yazılımdır. I2P'de anonim olarak e-posta servisini kullanabilir, sörf yapabilir, blog ve forum hizmetlerinden yararlanabilir, sitenizi yayımlayabilir, anlık mesajlaşma yapabilir (IRC), dosya paylaşabilir veya yükleyebilirsiniz. Tüm veriler birkaç katmandan oluşan şifreleme ile paketlenir ve tüneller ile iletilir. Bu yüzden I2P ile

56 http://yesilgazete.org/blog/2014/02/06/internet-yasagi-meclisten-gene-kurulunda-kabul-edildi/
57 https://network23.org/kame/2013/10/14/tora-giris/
58 http://geti2p.net/en/

ilgili bilinmesi gereken en önemli noktalardan biri “**tünel**” kavramıdır. I2P’deki bir tünel yönlendiriciler listesinden seçilen bir yoldur. Katmanlı şifreleme kullanılır ve böylece yönlendiricilerden herbiri sadece bir katmanın şifresini çözer. Şifre çözümü sonunda elde edilen bilgi, şifreli bilginin iletileceği bir sonraki yönlendiricinin IP adresidir. Bununla birlikte, her tünelin bir başlama noktası (*ilk router*) ve bir de bitiş noktası (*son router*) vardır. Ayrıca, gönderilen bir mesaj sadece tek yönlüdür. Eğer bu mesaja cevap verilecekse, yeni bir tünel üzerinden yapılacaktır.

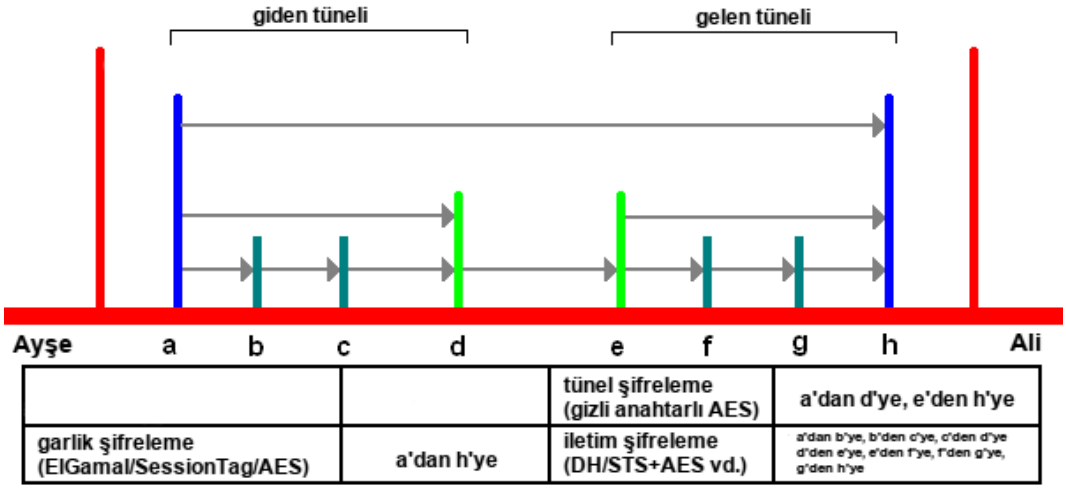
I2P’de iki çeşit tünel mevcuttur. Bunlar, tüneli oluşturan tarafından gönderilen mesajları içeren “**outbound**” (*giden*) ve mesajları almak için tünel oluşturan “**inbound**” (*gelen)*’dur. Bu iki tünelin bir araya gelmesiyle kullanıcılar birbirleriyle iletişim kurabilmektedirler. Şimdi bunu bir şema üzerinde görelim (*şemalar i2p‘den alıntıdır*[59]):

59 http://geti2p.net/en/docs/how/intro



Örneğimizde Ayşe Ali ile buluşmak istemektedir. Bunun için de ona "**Bugün buluşalım mı?**" diye bir mesaj gönderecektedir. Şemada gördüğünüz gibi her giden ve gelen tünelleri (*1, 2, 3, 4, 5 ve 6*) 2 sıçramaya sahiptirler. Bu sıçramalar peer'ler (*eşler*) üzerinden gerçekleşecektir. Sıçrama sayısını Eşler bölünden ayarlayabilirsiniz. Tıpkı torrentte olduğu gibi bağlandığınız birçok eş olacaktır. Bunlar I2P'nin ağ veritabanı (*network database*) içinde Kademlia algortiması ile bulunur. Ayrıca, sol ana menüde ve altta Shared Clients (*Paylaşılmış*

İstemciler)'den ayrıntılı bilgiye ulaşabilirsiniz. Ayşe, Ali'ye mesajını gönderdiği zaman pembe renkli olan giden tüneli üzerinden 3 veya 4 numaralı tünel geçidini kullanarak Ali'nin yeşil renkli gelen tüneli ile mesaj Ali'nin yerel istemcisine ulaşacaktır. Eğer, Ali bu mesaja "**Evet, nerde?**" diye cevap verecek olursa yeni bir tünel oluşturulacak, bu sefer de Ali'nin pembe renkli olan giden tüneli üzerinden 1 veya 2 numaralı tünel geçiti kullanılarak Ayşe'nin yeşil renkli gelen tüneli ile yerel istemcisine ulaşacaktır. Mesajın iletimi sırasında bir katmanlı şifreleme mevcuttur. Bir de katmanlı şifreleme nasıl oluyormuş ona bakalım:



Örneğimizde Ayşe'den Ali'ye "**Bugün buluşalım mı?**" mesajının gönderildiğini söylemiştik. Birinci katmanda mesajın ilerleyeceği tüm tünel (*a'dan h'ye*) garlik şifreleme ile şifrelenmiştir. Ayrıca, ikinci katmanda giden tüneli (*a'dan d'ye*) ve gelen tünelleri (*e'den h'ye*) bundan bağımsız olarak AES ile şifrelenmiştir. Bununla birlikte, üçüncü katmanda iletim esnasında her sıçrama (*a'dan b'ye, b'den c'ye, c'den d'ye, d'den e'ye, e'den f'ye, f'den g'ye ve g'den h'ye*) da şifrelenmiş

durumdadır. Bir saldırgan eğer bu mesajın içeriğini öğrenmek istiyorsa tüm bu katmanların şifreleri kırmak zorundadır. Şifreleme ile ilgili ayrıntılı bilgiye buradan ulaşabilirsiniz. Kafamıza bu kısım oturduysa artık kuruluma geçebiliriz.

Kurulum

I2P platform bağımsızdır. Burada anlatacağım GNU/Linux üzerinde nasıl kurulacağıdır. Kullanım olarak platform farketmiyor. Sisteminizde OpenJDK[60] kurulu olursa iyi olur. Değilse paket yöneticinizden kuruverin. Debian/Ubuntu türevi dağıtımlar kullanıyorsanız bir terminal açın ve:

Ubuntu için;

kame ~ $ sudo apt-add-repository ppa:i2p-maintainers/i2p

kame ~ $ sudo apt-get update

kame ~ $ sudo apt-get install i2p

Debian için;

kame ~ $ sudo nano etc/apt/sources.list.d/i2p.list

Aşağıdaki repo adreslerini yapıştırıp kaydedin:

deb http://deb.i2p2.no/ stable main
deb-src http://deb.i2p2.no/ stable main

60 http://openjdk.java.net/

kame ~ $ sudo apt-key add debian-repo.pub

kame ~ $ sudo apt-get update

kame ~ $ sudo apt-get install i2p i2p-keyring

Elle kurmak isterseniz önce şu adresten[61] "**jar**" paketini indirin ve bir terminal açın:

kame ~ $ java -jar i2pinstall_0.9.10.jar

Kurulumu gerçekleştirin. Hepsi bu kadar.

Kullanım

Hangi dizine kurulumu gerçekleştirdiğinizi bilmiyorum. Ben varsayılan olarak **/home/kullanıcı/i2p** dizini (*bende kullanıcı kame*) üzerinden gideceğim. Öncelikle i2p'yi çalıştıralım. Repolardan paket olarak kurduysanız servis yöneticiniz (*openrc, systemd vd.*) otomatik olarak eklemiştir. Eklememiş, çalıştırmamış vs ise:

kame ~ $ sudo /etc/init.d/i2prouter start

kame ~ $ sudo systemctl start i2prouter.service

Elle kurulum yaptıysanız:

kame ~ $ cd /home/kame/i2p

kame ~ $ sh i2prouter start

61 http://geti2p.net/en/download

I2P çalışmaya başladığı zaman varsayılan tarayıcınız hangisiyse onda I2P Router Console sayfasını açacaktır. Aşağıda Local Services kısmını göreceksiniz. Buradan isterseniz Configure Language ile dilini (**eksik çeviri**) Türkçe yapabilirsiniz. Bizleri ilgilendiren ilk kısım ağ durumudur. Birkaç dakika içinde sizlere "**OK (Tamam)**", "**Firewalled (Güvenlik duvarı engeli)**", "**Hidden (Gizli)**" vs gibi bir şekilde geri dönecektir. Bu ana sayfadaki sol kutu içinde görebilirsiniz. Eğer uyarı alıyorsanız güvenlik duvarınızda "**17193**" UDP portunu açabilirsiniz. Örneğin:

```
kame ~ $ iptables -A UDP -p udp -m udp --dport 17193 -j ACCEPT
```

Ağ durumumuz "**Tamam**" ise kullanım kısmını ben üç bölümde anlatacağım. Bunlar:

1. Internete I2P üzerinden anonim olarak çıkmak ve Eepsitelere erişmek
2. Anonim torrent kullanmak
3. Anonim e-posta almak

Internete I2P üzerinden anonim olarak çıkmak ve Eepsitelere erişmek

Önce, **I2PTunnel** (*I2PTüneli*) içinde tanımlı olan tünelleri başlatabilir veya durdurabilirsiniz. Http, https, IRC veya e-posta istemcisi gibi hazır tüneller göreceksiniz. Ayrıca, yeni bir tünel oluşturma işlemini de buradan yapabilirsiniz. I2P kullanımıyla ilgili detaylı bilgilere **Logs** (*Günlük*), **Stats** (*İstatistik*) ve **Graphs** (*Çizelgeler*) üzerinden ulaşabilirsiniz.

Eepsites (*Eepsiteler*), tıpkı Tor'daki[62] Hidden Services gibi I2P ağı içinden erişilen sitelerdir. Birçok konuda ve içerikte sitelere buradan erişebilirsiniz. Ayrıca, kendiniz de bir eepsite hazırlayıp, yayımlayabilirsiniz. Bunun için Local Services kısmından Websites'e girerek gerekli bilgileri alabilirsiniz.

Tarayıcınız için en kolay çözüm FoxyProxy[63] kullanmak olacaktır. FoxyProxy eklentisini kurduktan sonra HTTP için **Options -> Add New Proxy** diyorsunuz. Bununla birlikte, i2p ile Internete Tor ağı üzerinden çıkmaktasınız. i2p'nin outproxy'si Tor ağı olarak ayarlanmıştır. Tarayıcınızdan kontrol etmek isterseniz https://check.torproject.org adresine girebilirsiniz.

Host or IP Address = 127.0.0.1
Port = 4444
HTTPS için Port = 4445

Ayrıca, tüm bunları Privoxy kurarak da halledebilirsiniz. Privoxy ayarı için (*/etc/privoxy/config*):

```
forward-socks5 / 127.0.0.1:9050 .
forward .i2p 127.0.0.1:4444
forward 192.168.*.*/ .
forward 10.*.*.*/ .
forward 127.*.*.*/ .
```

62 https://torproject.org/
63 http://getfoxyproxy.org/

Tarayıcınızı HTTP ve HTTPS için ağ ayarlarından 127.0.0.1, port 8118 olarak ayarlayıp kullanabilirsiniz. Hepsi bu kadar.

Anonim torrent kullanmak

I2P'nin kendi ait **I2PSnark** adında anonim bittorent istemcisi vardır. Farklı istemciler ile (*Azureus*[64]*, Transmission*[65] *vd.*) kullanabilirsiniz. Sizin dikkat etmeniz gereken I2P üzerinden I2P'ye ait olmayan torrentleri indiremeyeceğinizdir. Yani, kickass'ten kopyaladığınız bir magnet linkini I2PSnark ile indiremezsiniz. Fakat, I2PSnark ile I2P üzerinde dolaşımda olan her torrenti indirebilirsiniz. Zaten, Eepsiteler içinde torrent siteleri var. İçerikleri de çok kötü değil. **i2p planet** veya **DifTracker** ile bunlara erişebilirsiniz. Torrentin ve I2P'nin daha hızlı olmasını istiyorsanız bant genişliğini ve paylaşımı artırmanız gerekmektedir.

Anonim e-posta almak

I2P'nin **Susimail** adında kendi ait anonim bir e-posta servisi vardır. Servislerden buraya ulaşabilirsiniz. Dışarıdan (*clear web*) kendinize e-posta atacaksanız **i2pmail.org** kullanarak atabilirsiniz. Kendi sayfasında açıklamalar mevcut ama ben burada tekrar belirteyim, i2p hesabınızdan gerçek hesaplarınıza veya gerçek hesaplara e-posta atmamaya özen gösterin. Bunu anonimlik derecenizi azaltmamak adına yapmayın dediğimi de unutmayın.

Son birkaç şey

I2P kullanmak, I2P ile torrent indirmek ve bunlara istinaden

64 https://www.vuze.com/
65 http://www.transmissionbt.com/

anonimliğiniz tekrar sizin tehlike modelinizde dayanır. Kimsiniz ve kimden saklanıyorsunuz? Neden ve ne tür bir risk almayı hedefliyorsunuz? I2P ile gelen anonim bittorrent istemcisi Azuerus'a kıyasla daha güvenlidir. **I2P'ye ait yerel kimliğinizi kimseyle paylaşmayın.** Hızlı olmasını istiyorsanız bant genişliğini ve paylaşımı lütfen artırın. I2P'ye giriş biraz kısa gibi oldu. İlerleyen zamanda bunu detaylandıracağım. Sizler de indirip kurar ve kurcalamaya başlarsanız çok çabuk birkaç şeyi deneyebilir ve belirli bir yol katedebilirsiniz.

10. Haklarım Hakların Hakları

> *Abdullah Gül önüne konan Internet düzenlemesini "**bir iki husus vardı onlar da giderilecek**" yaklaşımıyla onayladı. Bir iki husus kısmını saymazsak benim beklentim de onaylayacağı yönündeydi. Bazen insan bir şeyin olcağını bildiği halde kendini aksine inandırır. Ben bunu yapmayı çok önceden bırakmıştım.*

Abdullah Gül[66] tarafından dün[67] onaylanan sansürcü, toptan gözetimci, fişlemeci Internet düzenlemesi muktedirin çıkarları için geriye kalan herkesin gizliliğine vurulmuş bir darbedir. Fakat, **gizlilik bir insan hakkıdır**. Açık toplumlar için bir gerekliliktir. **Gizlilik hakkı, bizi biz yapan şeylerle çevrili, bize ait bir alana sahip olma hakkıdır.** Sadece biz bu alanda kimlerin olacağını ve paylaşmak istediğimiz şeylerin kapsamını, niyetini ve zamanlamasını kontrol etmeye sahibiz. Gizlilik hakkı, insani gelişme için bir araçtır, kişinin bireysel kimliğini inşaa eder, kendini tanımasına yardımcı olur, yaratcılık ve öğrenme için gereklidir. Ayrıca, insanoğlunun otonomisini korumak anlamına da gelir.

Madde 20 – Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*

Gizlilik hakkı bizlere yapay bir ada oluşturur. Bu ada fiziksel veya sanal olsun, **bizler burada bir üçüncü gözün gözetimi altında**

66 https://twitter.com/cbabdullahgul
67 http://t24.com.tr/haber/abdullah-gul-internet-yasasini-onayladi/251397

kalmadan, herhangi bir sosyal baskıya uğramadan ve yaptığımız eylemlerin sorumluluğunu üstlenmeye zorlanmadan deneyler ve hatalar yapabiliriz. Kendimize ait yalnız kalabileceğimiz bir alana sahip olamazsak kendimiz için neyin doğru veya yanlış olduğuna bağımsız bir şekilde karar veremez, gerçek anlamda otonom insanlar olamayız. Bununla birlikte, **gizlilik hakkı insanların fiziksel ve akıl sağlıklarını korumalarına yardımcı olur**. Çünkü, oluşturulan bu yapay adalar insanların yüzyüze gelmek istemediği kişilere sahip değildir. Kişinin oynaması gereken sosyal rollere bu adada gerek yoktur. İnsan bu alanda tamamen kendisiyle veya sadece orada olmasını istedikleriyle başbaşa kalabilir.

Madde 22 – Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.*

Madde 24 – Herkes, vicdan, dinî inanç ve kanaat hürriyetine sahiptir.*

Bir demokrasideki en hassas konulardan biri de ifade özgürlüğüdür. B**ireyin kendini tanıması için ifade özgürlüğü olmazsa olmazdır, ifade özgürlüğü bir doğru arayışıdır**. Öncelikle, düşünce bir kişi, olay vs. hakkında görüş sahibi olmak ve zihinsel hüküm kurmaktır. Zihinsel hüküm şunu söyler; bu süreç bireyin kendi iç dünyasındadır ve başkası tarafından bilinemez. Düşünceler ise yazıyla, sözle, resimle, fotoğrafla, video vd. ile yansıtılır. **Özgürce düşünemeyen, düşüncelerine ait içeriklerin sansürlendiği bir ortamda birey bunun bir sonucu olarak kendini özgürce ifade edemez.** Gizliliğin olmadığı, sansürün ve gözetlemenin olduğu bir yerde bizler daha farklı davranmaya başlar, daha resmi bir tavır takınır,

dürüstlüğümüzden ödün verir ve ayıplanma, dışlanma, fişlenme vs. korkuları yüzünden kendimizi özgürce ifade edemeyiz. Ek olarak, kendimizi özgürce ifade edemediğimiz bir yerde inanç özgürlüğünden söz edilemez. Ayrıca, ifade özgürlüğünün zarar görmesi araştırma özgürlüğünü olumsuz yönde etkiler. Çünkü ifade özgürlüğünün engellenmesi açık bilgi akışını etkileyecek ve böylece planlı ve sistemli olarak toplanan veriler, yapılan analizler, yorumlar, değerlendirilmeler bundan dolayı zarar görecektir.

Madde 26 – Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.*

Madde 27 – Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir.*

Tüm bunların karşısında artık bazı alışkanlıklarımızı da değiştirmek zorundayız. Kapalı kaynak, bilim etiğinden yoksun, arka kapılara sahip herhangi bir yazılımın ve donanımın kullanılmasına karşı çıkmak gereklidir. Sırf alışkanlık diyerek GNU/Linux[68] görmezden gelinmemelidir. Elbette, kullandığınız veya işiniz için gerekli olan her uygulamayı bulamayabilirsiniz. Fakat, gündelik kullanımınızda hiçbir eksiği yoktur. Hatta işiniz için benzer uygulamalara bile sahip olabilmektedir. Diğer yandan, kriptografi artık olmazsa olmazdır. Birine

68 http://distrowatch.com/

bir şeyler söylemek veya göndermek isteniyorsa ve bu Internetin gözetlendiği, sansürlendiği, insanların fişlendiği bir ortamda yapılıyorsa bunu şifreleyerek yapmak, anonim, otonom servisler, dijital para (*BTC*[69] *vd*.) sistemleri kullanmak ve bunları desteklemek gerekmektedir.

Ayrıca, **yukarıda bahsettiğim haklarımı hiçbir hükümet, parti, şirket ya da büyük ve yüzsüz örgütlerin savunmasını istemiyorum.** Benim adıma konuşmaları, haklarımı savunuyor gibi yapmaları, sanki benimle birlikte aynı mücadeleyi veriyormuş gibi görünmeleri sadece kendi çıkarları içindir. **Amaçları** benim gizliliğime değer vermek ve bunun için mücadele etmekten çok **sahip olduğum bilgiyi elde etmek ve onu kontrol etmektir**. Ben bunun bir parçası veya aracı olmak istemiyorum. Bununla birlikte, yalanın doğru, doğrunun ise yalan olduğu şu dönemde bir insan dürüstlükten asla vazgeçmemelidir. Okurken denk gelmiş veya bir yerlerden duymuşsunuzdur; bütün insanlar yalancıdır. Fakat, ben buna inanmıyorum. Tıpkı saydığım haklar gibi dürüstlük de benim için önemlidir. Bir insan dürüst olmadıktan sonra tüm bu haksızlıklara karşı nasıl bir fark yaratabilir ki? Şunu da bir kez daha yinelemek zorudayım. Empati yapmalıyız. **Empati yapmayı öğrenmeliyiz**. Sizi etkilemediğini düşündüğünüz durumlarda bile, sansüre, fişlemeye, gözetime vd.lerine hangi dilden, dinden, etnik kimlikten vs. maruz kalan olursa olsun bu haksızlıklara karşı mücadele etmek gerekir. Empati ve dürüstlük bunu gerektirir.

Madde 28 – Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve malî teminat yatırma şartına bağlanamaz.*

69 https://en.wikipedia.org/wiki/BTC

Son olarak, bunu okuyanlara da bir mesajım var. Yazıyı okurken benim ruhsal dalgalanmalarımı hissedebilirsiniz. Bunu yazıyı da nasıl algılarsanız algılayın. Bir manifesto veya sıradan bir yazı. Fakat devamlı olarak; ben, benim için, bence desem de bu yazı ancak sizlerle birlikte bir fark yaratabilir ve sadece sizlerle bir anlam kazanabilir. Sadece devamlı olarak gördüğünüz “**Internet yasaklarını aşın**“, “**sansürden korunma rehberleri**“, “**şunu kullanın sansürü aşın**” ile değil, sizlerin sansüre, fişlemeye, gözetime her ne ve kime yapılırsa yapılsın karşı çıkarak başa çıkabileceğinizi unutmayın. Ben böyle olduğunu düşünüyorum.

* Türkiye Cumhuriyeti Anayasası

11. Suriye'den Türkiye'ye Internet Sansürü

Bütün diktatörler aynı yolu izler.

Suriyeli yetkililerin Internet kullanıcılarına ait trafiği monitörlemek ve filtrelemek için kullandığı Blue Coat SG-9000[70] proxylerinin tuttuğu 600GB'lık kullanıcı verisi 2011 yılının Ekim ayında Telecomix isimli hacktivist grup tarafından sızdırıldı[71]. Ardından da bu verilerle ilgili akademik bir analiz yapıldı. Analizin detaylarına çok girmeden Türkiye'nin jet hızıyla onaylanan yeni Internet düzenlemesi ile çok benzer yönlerinin olduğunu farkettim. Bu benzer yöntemler Suriyelilerin sansürü aşmak için kullandığı yöntemler kadar sansür yöntemlerini de içermekte.

70 http://bluecoat.com/products/proxysg
71 http://www.h-online.com/security/news/item/Syrian-internet-censors-log-files-released-1355276.html

Öncelikle ProxySG 9000‘nin[72] ne olduğunu açıklayalım. Blue Coat[73] isimli firmanın ürettiği **bu proxyler** birleşik güvenlik çözümleri için üretilmiş ve **kullanıcı kimliği denetimi, web filtreleme, denetleme, ssl ile şifrelenmiş trafiği görüntüleme[74], trafik yönetimi gibi web trafiği üzerinde tam bir kontrol olanağı sağlamakta olan araçlardır**. Ayrıca, ProxySG 9000′lerin bir tanesi 15000GB kapasitelidir. Makaleye göre Suriye’de bunlardan 7 tane varmış. Ek olarak, sansür sisteminin altında yatan ve gerçek bir sansür sistemi oluşturan bu teknolojiyi de dikkate almanın gerekli olduğunu düşünüyorum. Hatta, hiç ummadığımız bir yerde ProxySG 9000 bile görebiliriz

Suriye’deki sansür sistemine kısaca bakacak olursak:

1. **Kategori tabanlı filtreleme**: Blue Coat’ın proxysi ilgili URL’ye ilişkin her isteği kategorilendirmekte ve her kategori de farklı filtreleme kurallarına sahip olmaktadır.
2. **Karakter dizisi tabanlı filtreleme**: Bunu basitçe şöyle ifade edeyim: A; sansürlü URL’ler B’de erişime açık URL’ler. c karakter dizisinin sıkça A’da gözükmekte olduğunu farzedelim. c karakter dizisinin A ve B’de görülme sıklıklarının da bir sayısı olsun. Eğer A’da 1′den fazla ve B’de hiç gözükmezse A’dan tüm c dizisi içeren istekleri silerek c’yi sansürlü diziler listesine ekliyor.
3. **URL tabalı filtreleme**: Twitter’da bir profile erişimi engelleyeceksiniz. Bunun için gidip komple siteyi erişeme engellemek yerine o profile ait URL’ye erişimi engelliyorsunuz.

72 http://wikileaks.org/spyfiles/files/0/226_BLUECOAT-SGOS_CMG_4.1.4.pdf
73 http://bluecoat.com/
74 http://wikileaks.org/spyfiles/files/0/219_BLUECOAT-SGOS_5.3.x_SSL_Proxy_Reference_Guide.pdf

4. **Kelime tabanlı filtreleme**: Çeşitli kelime grupları (*haydar, mini etek, liseli gibi*) üzerinden bir filtreleme. Bu alışık olduğumuz bir yöntemdir. Tahminen TİB bu yöntemle Türkiye'de 36000 küsür siteyi engelledi[75].
5. **IP tabanlı sansürleme**: Doğrudan IP adreslerinin erişime engellenmesi. Yani kısaca ISS'lerin bu IP adreslerine gelen istekleri hiç ulaştırmaması da denilebilir.

Bu filtrelemeler sonucunda kullanıcının istekleri iki şekilde cevaplanmaktadır. Ya yapılan istek reddedilecek (erişim engellendi, access denied gibi sayfalar) ya da başka bir adrese (*... **sayılı kararla erişime engellenmiştir***) yönlendirilmektedir.

Dikkati çekeceğim noktalardan bir diğeri de Arap Baharı[76] yaşanırken Suriyeli yetkililer Şubat 2011'de Facebook, Twitter ve Youtube gibi sosyal ağlara erişimi engellememişlerdir. Bunun yerine bu siteler monitörlenmekte ve seçici olarak sansürlenmekteydi. Diğer bir deyişle DPI[77] gibi yöntemlerle trafiği gerçek zamanlı olarak incelenmişlerdir. Bununla birlikte, anlık mesajlaşma uygulamaları (*Skype*), video paylaşım siteleri (*upload.youtube.com, metacafe*), anti-sansür uygulamaları içeren siteler (*Tor vd.*), haber ve muhalefet siteleri de seçici olarak sansürlenen trafik içerisinde yer almaktaydılar.

Suriye'deki Internet sansürü yapısını alıp Türkiye'ye uyarladığımızda, yeniden düzenlenen 5651 sayılı kanunun beraberinde

75 http://engelliweb.com/kategoriler/
76 https://en.wikipedia.org/wiki/Arab_Spring
77 http://enphormasyon.org/

getireceği sansürle çok ciddi benzer noktalar içermektedir. Birincisi, Türkiye'de bu yeni düzenleme öncesinde seçici bir sansür vardı. Kelime tabanlı olarak filtreleme uygulanmaktaydı. Diğer taraftan IP tabanlı sansürleme de yapılmıştı. Şimdi, **yeni düzenleme ile URL tabanlı filtreleme geldi ve web trafiğinin gerçek zamanlı olarak incelenebileceği bir yapıya kavuşturuldu. İkincisi, bu şekilde Facebook veya Twitter gibi siteler direkt olarak erişeme engellenmeden, Türkiye'deki Internet kullanıcılarının bu sitelere olan trafikleri monitörlenebilecek ve böylelikle de kullanıcı profilleri** *-diğer deyişle fiş dosyaları-* **oluşturulabilecek**. Üçüncüsü, Türkiye tüm bunlara yasal bir zemin hazırlamakla beraber MİT geçmişli bir başkan ve koruma kalkanı ile TİB'i dokunulmaz yapmıştır. Son olarak da yeni MİT yasa tasarısı[78] bu dokunulmazlığı alıp bir korku-baskı-ölüm yapısına dönüştürecektir.

Erdoğan bir zamanlar Esad için kardeşim diyordu[79]. Daha sonra onu katil, diktatör Esed olarak anmaya başladı[80]. **Internet sansürü anlamında Türkiye'de yapılanlara baktığımızda Erdoğan Esad ile aynı yolu izlediğini kendi adıma söyleyebilirim.** Çünkü, Suriye'deki Internet sansür sistemi Türkiye'nin mevcut yapısına rahatça uyarlanmaktadır. Yapılan yeni Internet düzenlemesi de ortak noktaları çok açık bir şekilde göstermektedir. Umarım bir gün Suriye'de yaşanan trajediyi Türkiye'ye de uyarlamak zorunda kalmayız.

78 http://www.bianet.org/bianet/siyaset/153692-mit-taslagi-evrensel-hukuk-ve-insan-haklarina-tehdit?bia_source=rss

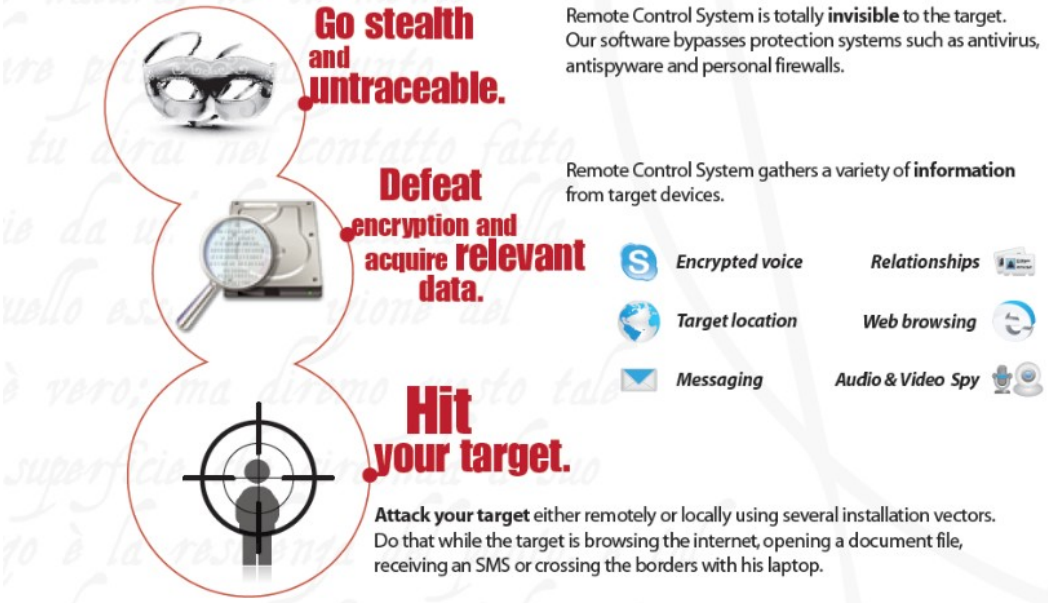
79 http://www.sabah.com.tr/Gundem/2009/12/23/suriye_ikinci_evimizdir

80 http://www.cihan.com.tr/news/Erdogan-Suriye-diktatoru-Esed-60-bin-insanin-olumune-sebep-oldu-CHOTMxMzYzLzQ=

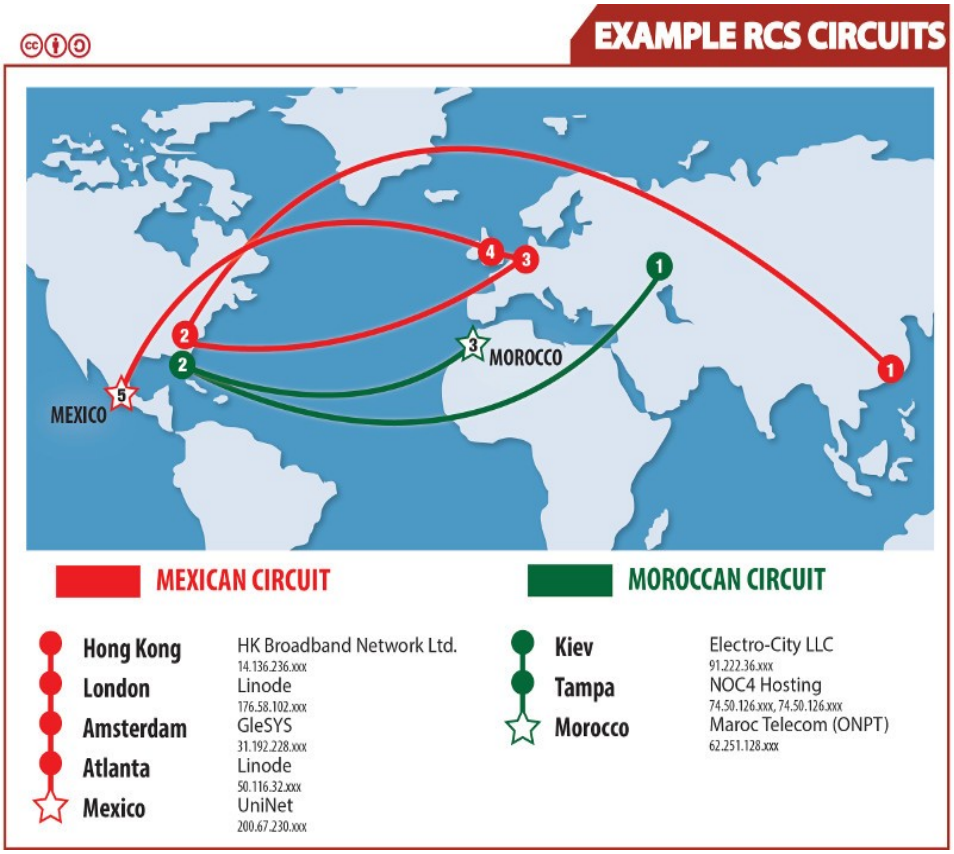
12. “İzi Sürülemeyen” Casus Yazılım ve Türkiye

> *Gün geçmiyor ki Türkiye’nin de içinde bulunduğu bir gözetleme sistemi orataya çıkmasın. Haklarımız o kadar büyük tehlike altında ki bunu hergün tekrar tekrar görüyorum.*

Milan’dan kısaca HT S.r.l olarak bilinen Hacking Team, devletler için “**saldırgan teknolojiler**” tedarik eden bir firma. Makalelerde geçtiği üzere ürünlerinden bir tanesi “**Remote Control System (RCS)**“, *-adı üzerinde-* uzaktan kontrol sağlayan bir trojan olup dünya çapında gizli servislere ve kanun uygulayıcılara satılmış. Hacking Team’in tanımladığı üzere bu trojan devletin kontrol edebildiği alanların dışında kalanlar ve şifreleme kullanları monitörlemek için geliştirilmiş. 2011 yılı RCS tanıtım broşürü:



Kısaca RCS hedef bilgisayar ve akıllı telefona girerek veri iletim için şifrelenmeden veya hiç iletilmemesi için müdahalede bulunuyor. Bununla birlikte, bir bilgisayarın harddiskinde bulunan dosyaları kopyalayabiliyor, Skype aramalarını, e-postaları, tarayıcıya girilen şifreleri (*keylogger gibi*) kaydedebiliyor[81]. Ayrıca, cihazın kamerasını veya mikrofonunu da kullanıcıyı gözetlemek ve dinlemek için aktif edebiliyor. **Hacking Team ise bu trojanı terör ve suçla mücadele etmek, siber soruşturmalar için oluşturduklarını, kesinlikle baskıcı rejimlere satılmayacağını/satmadıklarını söylüyor**[82]. İzi sürülememesine gelecek olursak hedefe yapılan saldırılar için kendine RCS sunucuları üzerinden tamamen farklı zıplama yolu hazırlamaktadır.



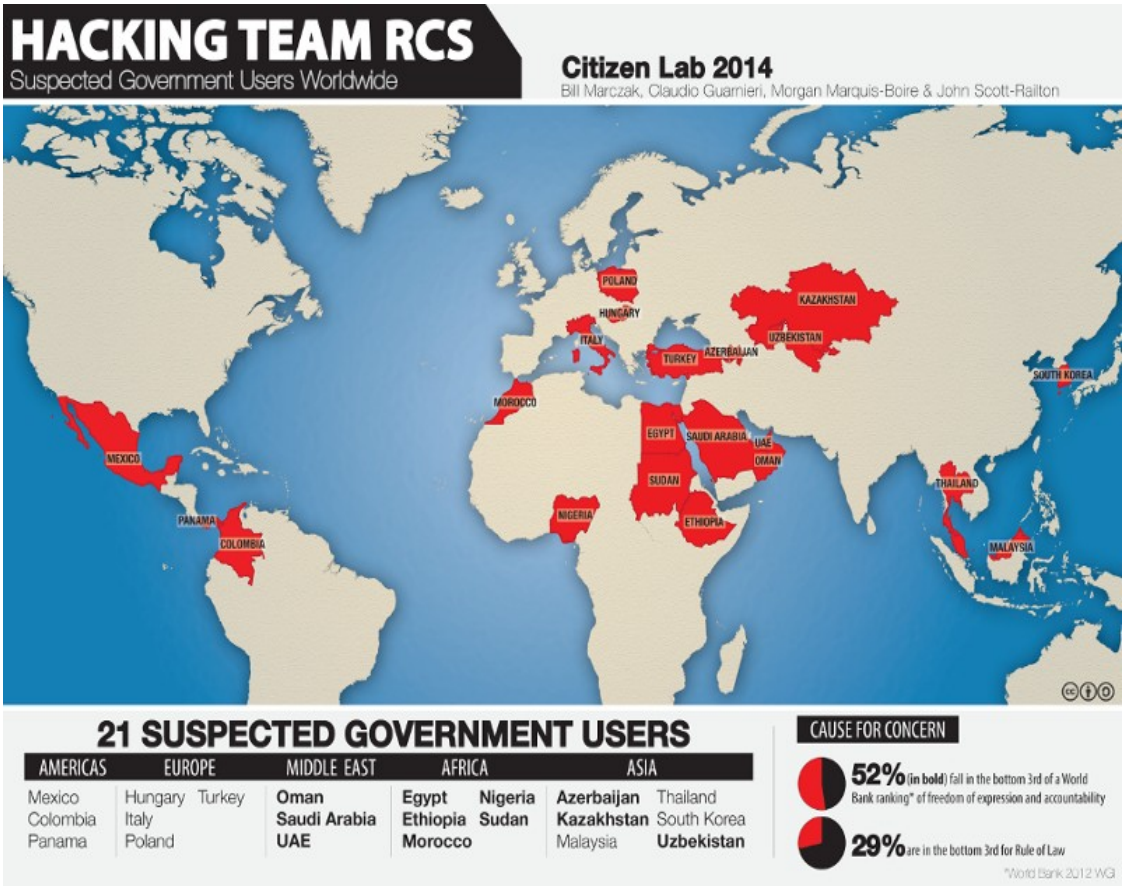
81 https://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam
82 http://news.cnet.com/8301-13578_3-57573707-38/meet-the-corporate-enemies-of-the-internet-for-2013/

Örneğin, RCS izinin sürülememesini sağlamak amacıyla Meksika'daki hedef için Hong Kong, Londra, Amstardam ve Atlanta üzerinden bir yol oluşturulmuş. Bir diğer örnek de Fas'taki hedef için oluşturulan Kiev ve Tampa yoludur.

İlk makale[83] Ethiopian Satellite Television Service[84] (*ESAT*) isimli, bağımsız ve Etiyopya diasporası üyelerine ait televizyon, radyo ve online haber kurumunu anlatıyor. ESAT kendini sürülen gazetecilerden, insan haklarını savunan, sivil toplum liderleri ve Diaspora üyelerinden oluşan bir yapı olarak tanımlamaktadır. Etiyopya'nın dikkati çeken bir diğer özelliği de Afrika çapında en çok gazetecinin mahkum edildiği bir ülke. Ayrıca, **Etiyopya devleti 1993'ten bu yana 75'ten fazla radyo ve televizyon kurumlarını kapatmış[85]**. ESAT'ın bir diğer özelliği ise Etiyopya hükümetinin muhalefet partilerini burada program yapmamaları için uyarmış olması[86]. ESAT tek bir saldırgan tarafından 2 saat boyunca hedef alınmış ve ESAT gazetecilerine RCS içeren rar, doc gibi dosyalar gönderilmiş. Bu örnekten çıkartılacak en temel sonuç, "**baskıcı rejimlere**" satılmadığı söylenen bu casus yazılımın bizzat baskıcı rejimler tarafından kullanıldığıdır.

İkinci makale[87] izi sürülemeyen bu casus yazılımın izini sürmeye çalışıyor. Kullandığı şüphelenilen ülkelerin haritası:

83 https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/
84 http://ethsat.com/
85 http://www.cpj.org/2013/11/ethiopia-arrests-2-journalists-from-independent-pa.php
86 http://ethsat.com/2014/01/09/udj-says-expressing-opinion-to-media-is-not-terror/
87 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/



Şüphelenilen ülkeleri sıralayacak olursak Meksika, Kolombiya, Panama, Macaristan, İtalya, Polonya, Türkiye, Umman, Suudi Arabistan, Birleşik Arap Emirlikleri, Mısır, Etiyopya, Fas, Nijerya, Sudan, Azerbaycan, Kazakistan, Malezya, Tayland, Güney Kore ve Özbekistan. Harita üzerinde de görülüğü gibi ülkelerin %52'si Dünya Bankası tarafından 3. dünya ülkesi olarak tanımlanmakta ve Türkiye de dahil olmak üzere baskıcı rejimlerin yönetimi altında bulunmaktalar. Tekrar Hacking Team'in ifadesine dönecek olursak **baskıcı rejimlere satılmayan bu casus yazılım bizzat bu rejimler tarafından kullanıldığından şüphelenilmiş**.

Makalede geçen RCS hedeflerine de kısaca bir bakacak olursak:

- Faslı yurttaş gazeteci grup Mamfakinch[88]
- Arap Emirlikleri'nden insan hakları aktivisti Ahmed Mansour
- Arap Emirlikleri'nden bir gazeteci ve bir insan hakları aktivisti

Makalede "**Bilinmiyor**" olarak geçen birkaç hedef daha mevcut. Bu durumun enteresan tarafı Hacking Team'in ısrarla Avrupa Birliği, Amerika, NATO ve benzer uluslararası organizasyonların baskıcı rejim, ifade özgürlüğünün kısıtlı, adalet sisteminin yozlaşmış, insan hakları ihlallerinin olduğu ülkeler diye adlandırdığı ülkelere kesinlikle tedarik edilmediğini söylemesine rağmen örnekler bunun tam tersini söylemekte, yurttaş gazeteci, insan hakları aktivistleri veya gazetecileri hedef alınmaktadır.

Türkiye bunun neresinde kısmına gelelim. Türkiye de sahip olduğu iktidar ile gayet baskıcı, hiçbir muhalefete tahammülü olmayan, kendi kıt anlayaşılarını hukuk diye dayatan polis devletinden muhaberat devletine geçmek için gün sayan bir devlet konumuna geldiğini biliyoruz. CitizenLab, RCS'nin proxy zincilerini 6 parmak izi (*fingerprinting*) üzerinden taramış ve bir sunucular listesi çıkartmıştır. Bu listeye[89] bakıldığında Türkiye'den (*firma ismi vermiyorum, whois çekin*) 1 Şubat 2014 tarihi itibariyle **176.216.47.175, 176.218.9.153, 176.55.188.147, 85.153.34.173, 85.153.34.187, 85.153.34.9 ve 95.9.71.180** adreslerine ulaşılmış. Bu adreslerle birlikte, ben de Türkiye'yi şüphelenilen (*kullanma potansiyeli yüksek*) ülkeler

88 http://slate.me/1eSTeUF
89 https://citizenlab.org/2014/02/appendix-list-servers/

kapsamına alırım.

Durumun vehameti açıkça ortada. Siber soruşturmalar için -sözde- izi sürülemeyen bir casus yazılım ve bu yazılımla insan haklarının ihlal edildiği ülkelerde muhalefet, gazeteci ve aktivistleri hedef alan rejimler. Diğer yanda para için gözetleme/takip yazılımları hazırlayanlar. Yakınlarda çıkan Internetten illegal mp3 indirenleri tespit edecek casus yazılım haberi de şu bahsi geçen iki makaleye tam oturmuyor değil. Türkiye birçok alanda geri kalmış bir ülke olabilir fakat gözetleme, takip, sansür ve fişlemede teknolojiyi hiç kaçırmıyor gibi duruyor.

13. URL Tabanlı Engelleme

Çalmayı iyi bildikleri gibi sansür ve gözetimi de iyi biliyorlar.

Dün gece Tayyip Erdoğan ile oğlu Bilal Erdoğan arasında geçen telefon konuşmalarına ait ses kaydı Youtube[90] üzerinden yayımlandı. Ses kaydı gerçek mi değil mi diyorsanız veya bu konuyla ilgili bir bilgi almak isterseniz Kıvaç Kitapçı'nın yazdığı "**Tayyip Erdogan – Bilal Erdogan Telefon Gorusmesi Analizi**" adlı makaleyi okuyabilirsiniz[91]. Dün geceye tekrar dönecek olursak, kayıt yayımlandıktan bir süre sonra erişime engellendi. Fakat her zaman alışık olduğumuz yöntemlerin aksine sayfaya "**http**" üzerinden eriştiğinizde tarayıcınızdan sanki öyle bir sayfa yokmuş, bağlantınız resetlenmiş gibi hata aldınız. Tahmin edildiği üzere bu URL tabanlı bir engelleme idi. Bu engelleme nasıl yapıldı ve engelin kaynağı neresidir üzerine küçük bir analizi kısaca fakat -olabildiğince- anlaşılır bir dille nasıl yapıldığını açıklayayım:

- Öncelikle, tcpdump[92] çalıştırıldı ve trafiğe konu olan veri paketlerine monitörleme yapılıp herhangi bir şüpheli durum var mı, varsa neden kaynaklanıyor bu belirlenmeye çalışıldı.
- dig[93] ile www.youtube.com adresinin DNS kayıtlarına bakıldı.
- traceroute[94] ile www.youtube.com adresine hangi sunucu veya yönlendiriciler üzerinden gidiliğine bakıldı.
- Tarayıcıdan ilk olarak URL tabanlı engellenen Youtube sayfasına

90 https://www.youtube.com/watch?v=Cvf4aeRLu0E
91 http://kivanckitapci.wordpress.com/2014/02/25/tayyip-erdogan-bilal-erdogan-telefon-gorusmesi-analizi/
92 https://en.wikipedia.org/wiki/Tcpdump
93 https://en.wikipedia.org/wiki/Dig_(command)
94 https://en.wikipedia.org/wiki/Traceroute

girildi.

- Ardından da açık olan -*yani engellenmemiş*- bir Youtube sayfasına girildi.

Açık olan Youtube videosuna erişim sonucu:

00:20:17.299332 IP (tos 0x0, ttl 48, id 63155, offset 0, flags [none], proto TCP (6), length 60)
fa-in-f93.1e100.net.http > 192.168.2.25.48657: Flags [S.], cksum 0xd7b8 (correct), seq 1852958477, ack 1827879094, win 42540, options [mss 1430,sackOK,TS val 1082331416 ecr 67618,nop,wscale 6], length 0

URL tabanlı engellenen Youtube videosuna erişim sonucu:

00:20:17.325219 IP (tos 0x0, ttl 30, id 0, offset 0, flags [DF], proto TCP (6), length 62)
fa-in-f93.1e100.net.http > 192.168.2.25.48657: Flags [R.], cksum 0x3cf3 (correct), seq 1:23, ack 375, win 229, length 22 [RST x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00]

Bu iki Youtube sayfasına ait tcpdump çıktısının en temel noktası, URL tabalı engellenen sayfanın TTL[95] (*yaşam süresi*) değeri açık sayfaya göre gelen değerden farklı. Bu fark şunu ifade ediyor; URL tabanlı engelleme yapılabilmesi için İSS'lerde IPS[96] gibi bir sistemin olması gerekli. Bu sistem ağı monitörleme, istenmeyen aktiviteleri tespit etme, bu aktiviteleri loglama, engelleme veya durdurma ve raporlama işlerini yapmaktadır. URL tabalı engellemenin çalışma sistemi de aynen monitörleme, loglama, engelleme ve erişimleri raporlama üzerinedir. Engelli sayfa çıktısında görüldüğü üzere İSS araya girerek TTL değerini

95 https://en.wikipedia.org/wiki/Time_to_live
96 https://en.wikipedia.org/wiki/Intrusion_prevention_system

değiştiriyor. Açık sayfada ise İSS tarafından bir müdahalede bulunulmadığı için TTL değeri normal düzeyde, yani gelmesi gereken düzeyde geliyor. Diğer yandan (*çıktı olarak vermedim*) traceroute sonucuna bakıldığında sorgu Google'a gidiyor. ICMP paketinin zaman aşımına uğradığı IP adresi **209.85.251.24**, yani Google ağı içinden. Herhangi bir sorun yok gibi duruyor. Peki tüm bunlardan ne anlamalıyız?

İSS, bir IPS kullanmakta ve IPS de bu mevcut URL tabanlı engellemeyi gerçekleştirmektedir. Bunu da RST (*reset*) paketi ile istemciye "**bu iletişimi kes**" mesajı vererek yapmaktadır. O gördüğünüz "**sayfa bulunamadı**" hatasını da bu yüzden almaktasınız. Ayrıca, RST paketi sunucu tarafından gönderilmemekte ve IPS bunu "**istemci engelli bir sayfaya erişmekte, ben de bunu durdurayım**" şeklinde görmektedir. Anlaşılan çalmayı öğrendikleri kadar sansür ve gözetimde de bilgi sahibi olmuşlar gibi duruyor. Fakat, bu sonuç sansürün ana kaynağını malesef söyleyemiyor. Bakalım, ilerleyen süreçte yapılan engellere de analiz yapmaya devam edip sansürün ana kaynağına ulaşabilecek miyiz zaman gösterecek. Bakarsınız, bu sürede belki sansürleyecek bir hükümet de kalmaz. Kim bilir.

Son olarak, bu yazı da montaj. TTL lobisi yazdı.

14. Tarayıcılar ve Eklentiler

> E-postalar üzerinden de bu sorular devamlı sorulduğu için kısa bir rehber hazırladım. Umarım işinizi görür.

İlk olarak belirtmeliyim ki bu rehberin %100 anonimlik veya güvenlik sağladığı yanılgısına kapılmak veya burada yazan tarayıcı ve eklentileri kullanarak gizliliğin sağlandığı, anonim kalındığı ve güvenli olunduğu kullanıcıyı büyük riskler içine çekebilir. Bu kavramların içi iyi bir şekilde doldurulmadığı sürece, bir tarayıcıdan veya eklentiden bir şeyler beklemek hata olur. Buraya kadar her şey anlaşıldıysa bana sıkça sorulan sorulara geçelim.

Hangi tarayıcıları kullanıyorum?

- Firefox Aurora
- Tor Browser

Neden Firefox Aurora ve Tor Browser kullanıyorum?

Öncelikle bu iki tarayıcıyı şu şekilde ayıralım: Firefox Aurora benim anonimliğe ihtiyaç duymadan, güdenlik işlerimi yüksek bir güvenlik sağlayarak gerçekleştirdiğim, eklenti desteği yüksek, stabil ve hızlı bir tarayıcıdır. Diğer yandan Tor Browser, anonim kalmamı sağlayan ve bunu en iyi şekilde yapan, benimle ilgili, gerçek kimliğime veya trafiğime ait en düşük bilgiyi sızdıran (*İSS trafiğinizi şifreli bile görse %100 anonimlik diye bir şey yoktur!*) bir tarayıcı olup, anonimliğe ihtiyaç duyduğum zamanlarda kullandığım diğer tarayıcıdır. İki tarayıcının kullanım amaçlarını ayırdıktan sonra diyeceğim bir diğer şey de, evet Firefox Aurora veya Google Chrome veya Opera veya başka bir

tarayıcı da Tor ağı üzerinden Internete çıkabilir. Fakat, anonimlik açısından bakarsak Firefox'un Tor ağı üzerinden Internete çıkması sizinle ilgili belirleyici bir bilgi sızdırır. Kaldı ki çeşitli ayarları (u*seragent vs*) değiştirseniz dahi sizinle ilgili bilgi toplayan servisler Tor Browser'dan farklı bir tarayıcı kullandığınızı parmak izleri (*fingerprinting*) üzerinden görebilir.

Hangi eklentileri kullanıyorum?

Tor Browser; HTTPS-Everywhere, Tor Button ve NoScript eklentileri ile birlikte gelmektedir. Bunun dışında başka bir eklenti kurmaya gerek yoktur. Diğer yandan, kurulacak eklentilerin anonimlik derecesini etkileme olasılığı da mevcuttur. Tor Browser'ı olduğu haliyle korumak en iyisidir.

Firefox Aurora için kullandığım eklentileri ve özelliklerini sıralayarak ilerleyeyim.

Adblock Edge

Adblock Edge[97], Adblock Plus'ın forklanmış halidir. Kendi tanımında da yazdığı üzere farkı; Plus -*muhtemelen*- maddi kazanç sağlamak için bazı reklamlara (*acceptable ads*) izin vermektedir, Edge'de ise izin yoktur.

Cryptocat

Tarayıcı üzerinden şifreli ve gizli mesajlaşmak ve sohbet (*OTR*) için -*şimdilik*- en iyi eklenti[98]. Ayrıca, grup özelliğine sahip olduğu için

97 https://addons.mozilla.org/en-US/firefox/addon/adblock-edge/
98 https://addons.mozilla.org/en-US/firefox/addon/cryptocat/

birden fazla kişi ile bir grupta toplu yazışma yapabilirsiniz. Bilinmesi gereken en temel şey, Cryptocat kullanırken IP adresiniz gizlenmiyor ve bu yüzden takip edilebilme olasılığınız vardır. Tor ağı üzerinden Cryptocat kullanarak bunu da aşabilirsiniz. Bunun için custom server'dan Tor Hidden Service'i seçebilirsiniz.

FoxyProxy Standart

Eğer tarayıcı üzerinde bir proxy yönetimi ihtiyacı duyuyorsam bunun için kullandığım tek eklenti[99]. Proxy yönetimi ile kastettiğim gerektiğinde örneğin Tor, i2p gibi proxyler veya sahip olduğum shell hesabı ile ssh tünel için kullanmaktır.

HTTPS-Everywhere

Birçok website https yapısına sahip olsa bile ziyaretçileri http üzerinden karşılamaktadır. Bu eklenti[100] ise güvenli olmayan http bağlantısını *-eğer website sahipse-* https olarak yeniden yazar ve kullanıcıları şifreli bir bağlantı ile karşılamaya zorlar. Olmazsa olmazdır. Bunun örneğini çok yakınlarda bir Youtube videosuna yapılan URL tabanlı engeli[101] aşmada ne kadar işe yaradığını görmüştük. Fakat tek sıkıntı, hala ve ısrarlar birçok website https kullanmamakta ve SSL sertifikası için para ödememektedir. Ayrıca, tavsiye olarak SSL Oberservation özelliğini aktif edin. Bu sizlere eğer bir man-in-the-middle[102] saldırısı varsa bilgi verecek ve eklentinin daha iyi geliştirilmesi için EFF'ye[103] anonim rapor gönderecektir.

---

99 https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/
100 https://www.eff.org/https-everywhere
101 https://network23.org/kame/2014/02/26/url-tabanli-engelleme/
102 https://network23.org/kame/2013/10/04/ssl-man-in-the-middle-ve-turktrust/
103 https://eff.org/

Mailvelope

Tarayıcı üzerinden OpenPGP[104] şifreli e-posta göndermek için -*bence*- en iyi eklenti[105]. Grafik arayüzü, hazır gelen servisler (*Gmail, Yahoo vs.*), anahtar yönetimi ile son kullanıcıya yönelik ve bu işi de en basit şekilde yerine getiriyor. Artık günümüzde şifreli e-posta göndermek bir zorunluluk olduğu için denenmesinde fayda var.

NoScript

Websiteleri üzerinde gelen JavaScript, Java, Flash, Silverlight ve diğer çalıştırılabilir eklentilerin kontrolünü ve iznini kullanıcıya bırakarak bu eklentilerden gelebilecek veri toplama ve saldırıları engeller. Hatırlarsanız, Freedom Hosting baskını sonrası zararlı bir JavaScript bulunduğundan[106] Tor Browser'ın bundan etkilendiği -*kısa süre içinde bu durum düzeltildi*- sözedilmişti.

RequestPolicy

Bunu kısaca şöyle anlatayım; bir websiteye herhangi bir makaleyi okumak için girdiniz, bu site üzerinde sunulan içerik olarak bir Youtube videosu da var, bu videoyu izlemeseniz dahi tarayıcınız Youtube'dan gelen isteği yanıtladı, ayrıca bir de Analytics mevcut. Böylelikle Google, Analytics ve Youtube ile sizin girdiğiniz siteyi ve okumak istediğiniz makaleyi, bu site üzerinde ne kadar vakit harcadığınızı öğrenerek sizin profilinizi çıkarmaktadır. RequestPolicy ise bu websitelerden gelen istekleri otomatik olarak engelliyor. Yönetim işini kullanıcıya bırakıyor. Diğer yandan XSS[107] veya CSRF[108] gibi saldırıları da bu şekilde

104 https://network23.org/kame/2013/08/28/pgp-kullanin/
105 http://www.mailvelope.com/
106 https://network23.org/kame/2013/10/14/tora-giris/
107 https://en.wikipedia.org/wiki/Cross-site_scripting
108 https://en.wikipedia.org/wiki/Cross-site_request_forgery

engellemektedir. NoScript ile birlikte müthiş bir ikili oluşturur.

Secret Agent

Uzun zamandır Cookieless Cookies[109], yani çerezsiz çerezler (*tercüme benim*) nedir, bir sayfayı çerezler ve JavaScript kapalı, VPN üzerinden ziyaret ettiğiniz zaman bile bu yöntemle takip edilebildiğinizi anlatmak istiyordum. Nasip bu yazıya oldu. Kısaca Etag[110] (*entity tag*) kavramını açıklayayım. Etag, http'nin parçası olan bir protokol olup, bir URL'de gelen içeriklerin (*gif, jpeg, js vs*.) değişip değişmediğini doğrular ve her içeriğe özgü bir etag (checksum, sağlama toplamı) atar. Eğer URL'deki içerik değişmişse yeni bir etag atanır. Bir örnek vereyim; bir sayfaya girdiniz, sayfada bir jpeg var. Bu jpeg'in kendine ait bir etag'ı mevcut. Tarayıcı jpeg'i açtığı ve etag'ı öğrendiği zaman sunucuya doğrulama için bilgi gönderir. Sunucu jpeg'de bir değişklik olup olmadığını kontrol eder. Eğer yoksa jpeg'i yeniden almaya gerek kalmaz ve böylece gereksiz veri akışından kurtulunur. Ziyaretçilerin takibi ise bu yöntemle olmaktadır. Çünkü sunucu her tarayıcıya has bir etag verecek ve veritabanından da bunu kontrol edecektir. Bunu aşmada Self-Destructing Cookies'in yanısıra Secret Agent eklentisi de işe yaramaktadır[111]. Tarayıcının useragent'ını düzenli olarak değiştirerek devamlı farklı etag'ların oluşturulmasını sağlar ve bunlar üzerinden gerçekleştirilecek takibi aşmaya çalışır. Whitelist'e sahip, böylece güvendiğiniz websitelerini buraya ekleyebilir ve sorunsuz kullanabilirsiniz.

---

109 http://lucb1e.com/rp/cookielesscookies/
110 https://en.wikipedia.org/wiki/HTTP_ETag
111 https://www.dephormation.org.uk/index.php?page=81

Self-Destructing Cookies

Otomatik olarak kullanılmayan çerezleri temizleyen bir eklenti[112]. Ayrıca bir whitelist'e de sahip. Buraya güvendiğiniz websiteleri girerek diğer sitelerden gelen çerezlerin belirli bir zaman aralığında otomatik ve kalıcı olarak silinmesini sağlayabilirsiniz. Böylelikle farkında olmadan çerezler tarafından gözetlenmenin de önüne geçersiniz.

TinEye Reverse Image Search

Bir imajın sahte olup olmadığını anlamanın en iyi yolu bu eklentiden geçiyor[113]. Örneğin Twitter'da paylaşılan bir fotoğrafın o ana ait olup olmadığını merak ettiniz. Bu eklenti ile fotoğrafa sağ tıklayarak TinEye'ın devasa veritabanında aratabilir, daha önce kullanılmışsa hangi sitelerde ve ne zaman kullanıldığını görebilirsiniz. Dezenformasyona karşı ilaç gibi gelecektir.

WebPG

WebPG'de tıpkı Mailvelope gibi GnuPG/PGP şifreli e-postalar göndermenizi sağlayan gayet kullanışlı bir eklenti[114]. Bazı web arayüzleri ile sıkıntıları giderilebilmiş değil ama basit bir kullanıma sahip. Sisteminizde ekli olan size ve arkadaşlarınıza sahip tüm anahtarları otomatik olarak alıyor. Denemeye kesinlikle değer.

Vimperator

Vim kullanmaktan büyük keyif aldığım bir editör. Kısayolları çok sevdiğim için ve bunları da bir tarayıcı üzerinde fareye ihtiyaç duymadan rahat bir şekilde kullanabilmek için en iyi eklenti

112 https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/
113 https://addons.mozilla.org/en-US/firefox/addon/tineye-reverse-image-search
114 https://addons.mozilla.org/en-US/firefox/addon/webpg-firefox/

Vimperator[115]. Gerçi, VimFx[116], Vimium[117] ve Pentadactyl[118] gibi uygulamalar da mevcut. Hepsi de aynı işi yapıyor.

Tüm bunlar gizliliğim, anonimliğim veya güvenliğim için yeterli midir?

Hayır! Öncelikle gizlilik, anonimlik ve güvenlik gibi kavramlar doğru anlaşılmalıdır. Anlaşılmadığı takdirde kullandığınız araçlar elinizde bir çöpe dönüşür. Bu yüzden tekrar ve tekrar tavsiye olarak gizlilik, anonimlik gibi kavramların içini iyi doldurmak ve bu konularda bolca araştırma yapmak gerekiyor.

115 https://addons.mozilla.org/en-US/firefox/addon/vimperator/
116 https://addons.mozilla.org/en-US/firefox/addon/vimfx/
117 https://addons.mozilla.org/en-US/firefox/addon/vimium/
118 https://addons.mozilla.org/en-US/firefox/addon/pentadactyl/

15. Interneti Kapatmaya Doğru Giderken

Kendine gazeteci diyen 4 kişi; Rasim Ozan Kütahyalı, Mehmet Barlas, Mahmut Övür ve Erdal Şafak, atv'de canlı yayında Tayyip Erdoğan'la bir araya gelip gündeme dair soruları sordular ve sorulara yanıt aradılar. Konuşma beklediği gibi döndü dolaştı Internete düşen ses kayıtlarına geldi ve Erdoğan:

30 Mart'tan sonra atacağımız başka adımlar var. Bu konuda kararlılığımız var. Biz bu milleti Youtube'a, Facebook'a, bilmem şuraya buraya yediremeyiz. Atılması gereken adım neyse biz bu adımı en kesin hatlarla atacağız. Kapatılması dahil.

diyerek[119] ilerleyen süreçte gelecek website engellerinin de haberini vermiş oldu. Interneti "**sınırsız bir şey, engeli yok**" diyerek kendi denetimi altında tutmayı istemesi zaten şaşırtıcı bir şey değildi. Daha önce de bu konuyla ilgili olarak bir şeyler demişti diye hatırlıyorum.

Bununla birlikte, son günlerde yaşanan SSL sertifika hataları, Google'a ve birçok siteye erişimde sıkıntılar, Internet'in aşırı yavaş oluşu ben ve birçok kişide de bir şeyler üzerine çalıştıkları izlenimini uyandırdı. Yeni Internet düzenlemesi ile getirdikleri URL tabanlı engellemenin altyapısını muhtemel tüm İSS'ler için kullanılabilir olmasını sağlamaktaydılar veya muhtemel Erişim Sağlayıcıları Birliği'nin altyapısı için çalışmalar yapıyorlardı. Her şekilde bizler için hayırlı bir şeylerin olmadığı ortadır. Bugünkü açıklamadan sonra da

119 https://www.youtube.com/watch?v=Ix_i8i5TkVA

denedikleri sistem her ne ise başarılı bir sonuç alamadılar ve çok kullanılan ve paylaşımların döndüğü, haberlerin çok hızlı yayıldığı, Erdoğan'ın da zikrettiği bu websitelerin kapatılmasına -*dolaylı da olsa*- karar verdiler.

URL tabanlı engellemenin olduğu gün traceroute Youtube için olması gereken sonucu vermişti[120]. Google'da yaşanan SSL hataları ve erişim sıkıntılarının yaşandığı zaman baktığımda ise tarayıcıdan Google'a erişilse bile traceroute çıktısında zaman aşımlarının olduğu ve ICMP paketinin Google sunucularına ulaşamadığını farkettim. Bu şu anlama geliyor; traceroute'da paketler Google'a ulaşıp geri dönemiyor; belki de erişiyor fakat dönüş yolunda çeşitli sorunlarla karşılaşıyor. Bu sorunlar; bir güvenlik duvarı veya çeşitli güvenlik önlemleri tarafından bilinçi olarak bloklama olabilir, hop'larda ICMP kapalı olabilir, bloklama traceroute'u etkileyebilir fakat sunucu bağlantıları bundan etkilenmeyebilir.

```
traceroute to google.com (64.15.117.245), 30 hops max, 60 byte packets
 1  192.168.2.1 (192.168.2.1)  2.590 ms  4.451 ms  5.076 ms
 2  93.155.2.5 (93.155.2.5)  12.404 ms  13.838 ms  15.903 ms
 3  81.212.106.141.static.turktelekom.com.tr (81.212.106.141)  17.969 ms  19.386 ms  20.518 ms
 4  pendik-t2-1-pendik-t3-1.turktelekom.com.tr.221.212.81.in-addr.arpa (81.212.221.61)  22.794 ms  23.862 ms  25.339 ms
 5  * * *
 6  212.156.41.202.static.turktelekom.com.tr (212.156.41.202)  50.162 ms  28.137 ms  27.943 ms
 7  * * *
 8  * * *
```

120 https://network23.org/kame/2014/02/26/url-tabanli-engelleme/

9 * * *

10 * * *

Kısaca bu çıktıyı yorumlarsak (*30. hop'a kadar böyle, çıktı uzun diye 10'da bıraktım*.):

- Son erişilebilir sistem 6. hop'tur.
- Sorun 7. hop'ta olabilir ya da 6. ve 7. hop arasındaki bağlantıda olabilir.
- Bu sorun belki dönüş yolunda da olabilir. 6. ve 7. hop'lardaki istemcilerin farklı dönüş yolları olmasından kaynaklanıyor da olabilir.
- 7. hop'un dönüş yolunda bir sorun olduğu halde 6. hop'un dönüş yolunda herhangi bir sorun olmayabilir.
- Sorun bu sistemden kaynaklanabilir veya bu tamamen farklı bir sistem olabilir.
- İşin kötü tarafı bu sorun İSS'den kaynaklanan bir sorun da olabilir.

Bu analizin daha tutarlı olabilmesi için de birçok farklı noktadan buna benzer analizler yapılmalıdır. Bugün tekrar traceroute ve tcptraceroute yaptığımda paketlerin Google sunucularına ulaştığını gördüm. Bu, sanırım analizi desteklemesi açısından önemli bir nokta olsa gerek. Ek olarak, TCP/IP konusunda yeterli bilgiye sahip olmadığım için daha iyi analizler yapılırsa eğer lütfen bana ulaşın yazıya ekleyeyim. Bununla birlikte, İSS'den kaynaklanan bir sorun olabilir demiştim. Dikkat ettiyseniz İSS'den sonra paketler kayboluyor. Ayrıca,

bu sorundan ziyade gözetim ve erişim engelleri için bir donanımın kullandığı anlamına gelebilir. İSS'nin tek başına yazılımsal olarak böyle bir trafik yükünü çekmesi pek muhtemel gözükmediği için donanım üzerinde çalışan yazılımlar böyle "**sorunlar**"'a da neden olabilirler.

Öte yandan, bugün Lütfü Elvan'ın bir açıklaması oldu. Önemli noktaları buraya alıntılıyorum:

Sayın Başbakanımızın ifade ettiği husus şu: dünyanın hiçbir ülkesinde görülmeyen alçakça saldırılar var. Dünyanın hangi ülkesine gitseniz, bu ülkenin başbakanına, bakanlarına, ailesine, küfürler hakaretler, ağza alınmayacak ifadeler olmaz. Maalesef bunların hepsi internet ortamında yer alıyor. Dünyanın hiçbir ülkesinde bu tür uygulamaya müsaade edilmez... Böyle bir şey yok. Dünyanın hangi ülkesine giderseniz gidin, bu tür hususlarla karşı karşıya kalmak mümkün değil. Eğer böyle bir şey olsa, anında bunun engellenmesi yapılır. Düşünün Başbakan'a, Cumhurbaşkanı'na küfür edilecek, olmadık hakaretler yapılacak, yasa dışı bir takım görüntüler alınıp ve bunlar servis edilecek, bunları da biz içimize sindireceğiz. Böyle bir şey mümkün değil. Böyle bir şey olamaz...

Konunun tekrar dönüp dolaşıp ahlaki değerler üzerinden dayatılmaya çalışılan bir sansüre geldiğini gösteriyor. Elvan, dikkati çekecek çok önemli şeyler söylemiş, özellikle de anında bunun engellemesi yapılır kısmı ilerleyen sürecin bir habercisi gibidir. Ayrıca, Abdullah Gül; "**Facebook ve Youtube gibi platformların kapatılması**

söz konusu olamaz” dedi[121]. Fakat, o ne derse ben tam tersini düşüneceğim için bu açıklamasını da günü kurtarmak amaçlı olarak yorumluyorum. Erdoğan’ın bu çıkışı, üzerine söylenenler, aslında pek de tartışma yaratmadı. Diğer yandan, böyle bir algı yaratılmaya çalışıyor. Buna gündem değiştirme, hedef saptırma, oyalama ne derseniz diyin. 1 yıl daha iktidardalar. Yerel seçimleri kaybetmeleri bu açıdan çok bir anlam ifade etmiyor. Hatta bence yerel seçimleri kaybedersek yargılanırız veya bir şeyler değişebilir algısı da iğrenç geliyor. Son olarak, bu websitelerin kapatılması seçimlerde bir hilenin döneceği ve bunun da sosyal medya üzerinde en az şekilde duyurulması veya konuşulmasını istedikleri için 30 Mart tarihi özel olarak seçildi izlenimi uyandırmıyor da değil.

121 http://www.aljazeera.com.tr/haber/gul-kapatma-soz-konusu-olmaz

16. TİB ve Metadata

5651 sayılı Internet düzenlemesinin etkileri ve tepkileri sürerken, Gül'ün hiç şaşırtmayan bir hamleyle onayladığı ve birkaç sorunlu şey var düzeltilecek demesi ile hükümetten yana saf tuttuğunu bir kez daha ispatlamıştı. Cumhurbaşkanı danışmanı Yusuf Müftüoğlu The Wall Street Journal'a[122] "**Türk siyasetinin paranoyak tarzı**" makalesi[123] ile ilgili sitem dolu bir e-posta göndermiş[124]. Bu e-postada da özellikle dikkatimi çeken Gül'ün Internet düzenlemesindeki "**en tartışmalı maddelerin –global normlar ile en uygunsuz olanların– derhal değiştirileceği yönünde hükümetten güvence aldıktan sonra bu onayı vermiştir**" cümlesi oldu. Ayrıca, haberin başlığı da Gül'ün Internet yasasına direndiğini söylemektedir. Peki metnin devamında Gül'ün direndiğine dair bir ibare var mı? Yok ve daha kötüsünü belirtmişler. Adı da metadata!

Öncelikle, **metadata** nedir değildir? Kısaca, bir veri hakkındaki verilerdir. Bunu detaylandırırsak eğer, **belirli bir veri setine ya da kaynak hakkında nasıl, ne zaman ve kim tarafından oluşturulduğu hakkında tanımlayıcı bilgiler içerir**. Metadata çoğunlukla Internet içeriğine bir gönderme olsa da fiziksel veya elektroknik içerikler hakkında da olabilir. Ayrıca, bir yazılım veya elle oluşturulabilirler. Biraz daha ayrıntıya girelim, **bir metadata saat kaçta, nereden, hangi baz istasyonunu kullanarak kimi aradığınızı, arama yaptığınız telefonun IMEI numarasını, ne**

122 http://wsj.com.tr/
123 http://www.wsj.com.tr/article/SB10001424052702303795904579432692543546318.html
124 http://www.wsj.com.tr/article/SB10001424052702303802104579448652097975062.html?mod=wsj_share_tweet

kadar süre konuştuğunuzu vb. bilgileri içerir. Bunu Internet açısından düşünecek olursak, örneğin bir e-posta gönderdiniz, e-postalarınıza nereden eriştiğiniz, ne zaman eriştiğiniz, IP adresiniz, e-postada kullandığınız adınız, alıcının adı, zaman dilimi, yazı karakter kodu, sunucu transfer bilgisi gibi detaylı bilgileri içermektedir. İşin komik tarafı şu:

Son olarak, servis sağlayıcıları internet kullanıcılarının yalnızca üst verilerini (metadata) TİB'e verecek ve bu yalnızca mahkeme emri ile yapılabilecek. Önceki şeklinde, daha detaylı bilgilerin mahkeme emri gerektirmeksizin iletilmesi isteniyordu.

Sizin gizliliğinize ait tüm içerikler "**mahkeme emr**i" adı altında bir şekilde TİB'e verilebilecek. Bununla birlikte, metadata çok kapsamlı ve sadece tek taraflı bilgiler içermediği için sizinle birlikte iletişime konu olan karşı tarafa ait bilgiler de verilmiş olacak. Tabi ki bizler Internet kullanmasını bilmeyen ve gizlilik konusunda yeterince bilgi sahibi olmadığımız için bu açıklamayı da "**evet, kesinlikle çok haklısınız**" çerçevesinde değerlendiriyoruz. Üzülerek söylüyorum ki, açıklama yaptıkça daha çok batıyorlar ve şuna artık eminim, ne dediklerinin veya söylediklerinin ne anlama geldiğinden bile emin değiller.

Metadata ile ilgili meşhur bir örnek de Petraeus skandalıdır[125]. Bu skandal, CIA yöneticisi olan general David Petraeus[126] ile gazeteci ve

125 http://en.wikipedia.org/wiki/Petraeus_scandal
126 http://en.wikipedia.org/wiki/David_Petraeus

Amerikan ordusu istihbaratında görevli Paula Broadwell[127] arasındaki evlilik dışı ilişki ve konuya dahil birçok farklı kişiden oluşmaktadır. Kısaca, Paula ve David ortak bir anonim e-posta kullanarak birbirleriyle iletişim kurmaktadırlar. İkisi de e-posta göndermek yerine bu anonim e-postada yazdıklarını kaydedip okumaktalar. Paula, kamuya açık alanlardan Internete girip bu kayıtlı mesajları okur ve nerden, ne zaman okunduğuna ve oluşturulduğuna dair metadata verisi birikir. FBI'ın araştırması sonucunda da metadatalar ile Paula'nın kimliğine erişilir. Guardian'ın metadata'ya giriş makalesinde[128] metadata ile ne tür bilgilerin toplandığına dair detaylı bir anlatım mevcut. Buradan bazı şeyleri aktaracağım:

Kamera

- GPS bilgileri
- Oluşturulma ve düzenleme tarihi
- Fotoğrafa ait içerik bilgileri
- Kamera modeli
- Kamera ayarları (*flash, f-stop, shutter hızı vs.*)
- Fotoğraf özellikleri (*boyut vs.*)

Facebook

- Ad ve soyad, doğum tarihi, yer, iş, ilgi alanları gibi biyografi bilgileri

127 http://en.wikipedia.org/wiki/Paula_Broadwell
128 http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1111111

- Kullanıcı adı ve ID
- Abonelikler
- Cihaz bilgileri (*telefon, bilgisayar vs*.)
- Aktiviteler, beğeniler, etkinlikler
- Facebook etkinliğine dair zaman, saat ve saat dilimi

Twitter

- Ad, yer, profil bilgileri ve URL
- Hesap oluşturulma tarihi
- Kullanıcı adı ve ID
- Tweetlerin gönderildiği yer, zaman ve saat dilimi
- Tweetlerin ve cevapların ID’si
- Takipçiler, takip edilenler, favoriler
- Tweetlerin gönderildiği uygulama

Google Arama

- Arama sorguları
- Aramada çıkan sonuçlar
- Arama sonucu erişilen bağlantılar

Tarayıcı

- Ziyaret edilen sayfalara ait bilgiler ve zamanı
- Otomatik tamamla ile muhtemel giriş bilgileri ve kullanıcı verileri

- IP adresi, cihaz ve donanım bilgileri, işletim sistemi ve tarayıcı bilgisi
- Websitelerinden alınan çerez ve cache verileri

Neyse ki bizler teknolojinden anlamayan insanlarız ve bunların ne anlama geldiğini bilmiyoruz. Teşekkürler TİB, teşekkürler Müftüoğlu, teşekkürler Gül! Sayenizde Internet hiç olmadığı kadar “**özel hayatın ve iletişimin gizliliğine**” saygılı olmamıştı. Google’dan aratıp anaysayadan bir iki şey “**sallamak**” isterdim sizlere ama artık yazmaktan tiksiniyorum.

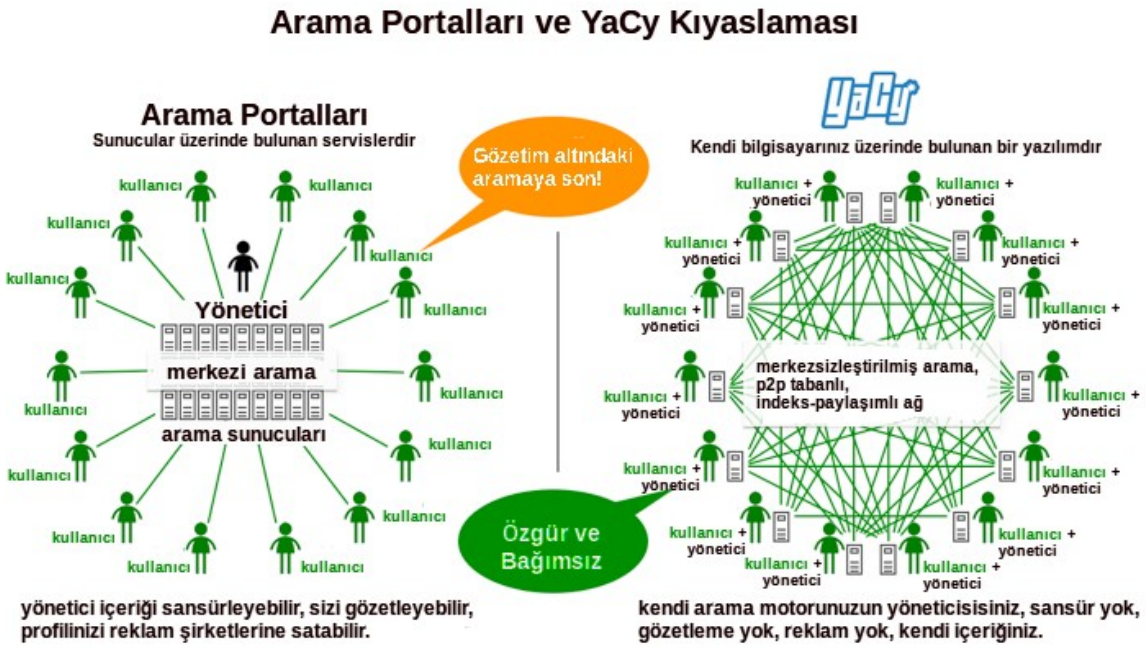
17. YaCy – P2P Arama Motorunuz

> Twitter'ın erişime engellemesi[129] ile ilgili mesajım için buraya[130] tıklayabilirsiniz.

YaCy[131], p2p mantığı üzerine kurulu ücretsiz, açık kaynak, özgür bir arama motoru yazılımdır. Genel olarak Java dili ile yazılmıştır ve platform bağımsızdır. Yani, illa GNU/Linux kullanmanıza gerek yoktur. P2P ağlarda olduğu gibi YaCy'de de birçok istemci vardır. Her YaCy-istemcisi birbirlerinden bağımsız olarak bir Internet sayfasını tarayabilir, analiz edebilir, sonuçları YaCY-istemcilerinin erişebilmesi için ortak bir indeks veritabanında tutup paylaşabilir. Tüm YaCy-istemcileri eşittir ve arama portallarında (*Google, Bing, Yandex vs*) merkezi bir sunucusu yoktur. Kısaca, YaCy için merkezsizleştirilmiş arama motoru da denilmektedir.

Merkezsizleştirilmiş Arama Motoru

129 http://bianet.org/bianet/siyaset/154327-twitter-i-kapatti
130 http://inciswf.com/gecmisinisikiyim.swf
131 http://yacy.net/en/



Özel mülkiyet bir arama motoru düşünün. Bir merkezi ve yönetici(*leri*) mevcuttur. Bu arama motorunun sizin kontrolünüz dışında olan özel sunucularının bir merkezi vardır, sizin aramalarınızla ilgili bilgi toplar, sonuçları çeşitli gerekçelerle (*telif vs.*) sansürleyebilir, sizin arama sorgularınız ve eriştiğiniz sonuçlarla ilgili profil oluşturup bunu reklam için kullanabilir veya satabilir. YaCy'de ise bu durum tamamen farklıdır. Öncelikle, böyle bir merkeze bağlı değilsiniz. Kendi arama motorunuzun hem yöneticisi hem de kullanıcısısınız. Diğer yandan arama portallarındaki gibi içeriğiniz sansürlenmez, yöneticiler tarafından gözetlenmez ve herhangi bir reklam yoktur. Kendi içeriğinizi oluşturabilir, istediğiniz siteleri indeksleyebilir ve 600'den fazla istemcinin düzenli olarak katkı yaptığı 1.4 milyardan fazla dökümana sorunsuz, herhangi bir engele ve kısıtlamaya takılmadan erişebilirsiniz.

Kurulum ve İlk Çalıştırma

İlk önce sistemimize Java kurmalıyız. Ardından YaCy'i kurabilir ve çalıştırabiliriz. Windows kullanıcıları buradan[132] MacOS kullanıcıları da buradan[133] indirip kurabilirler. Paket yöneticiniz ve dağıtımınız ne olduğunu bilmediğim için Debian türevi dağıtımlara uygun bir Java kurulumu gösterdim. Diğer kurulum ve çalıştırma dağıtım bağımsızdır.

```
kame - $ apt-get install openjdk-7-jre

kame ~ $ wget -c
http://yacy.net/release/yacy_v1.68_20140209_9000.tar.gz

kame ~ $ tar xzv yacy_v1.68_20140209_9000.tar.gz && mv yacy
~/.yacy

kame ~ $ cd ~/.yacy && sh startYACY.sh
```

Temel ayarlar

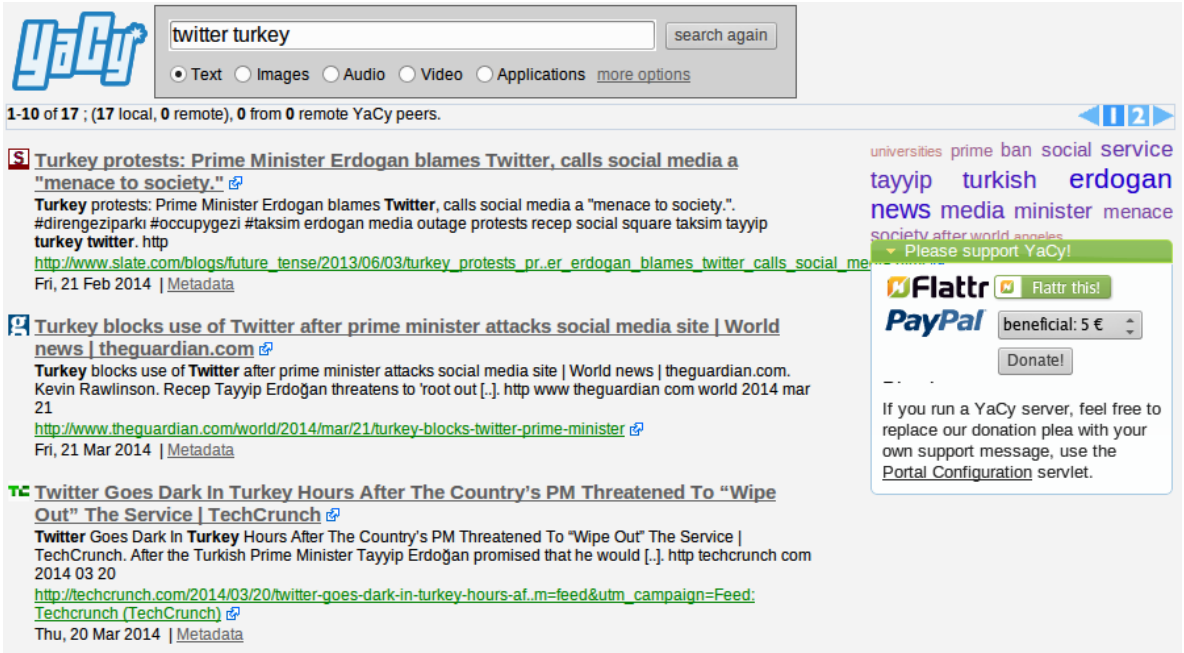
Tarayıcınızdan localhost:8090'a girdiğinizde[134] YacY'nin durum (*status*) ana sayfasını göreceksiniz. Şimdi ilk olarak yanındaki **Basic Configuration**'a tıklayarak bizi ilgilendiren birkaç ayarı yapalım. **1. seçenek dil seçeneği**. Buradan size uygun olan bir dili seçebilirsiniz. **2. seçenek kullanım amac**ı. Üç seçenek mevcut. İlki, topluluk tabanlı arama. YaCy-istemcileri üzerinden arama yaparsınız. İkincisi, YaCy'i diğer YaCy-istemcilerinden bağımsız olarak yapılandırır, kendi indekslediğiniz ve robotlarla taradığınız siteler üzerinde arama yapılacak şekilde yapılandırabilirsiniz. Üçüncüsü, kendi ağınız ve siteniz için bir arama moturu oluşturabilirsiniz. **3. seçenek kullanıcı adını**z.

132 http://yacy.net/release/yacy_v1.68_20140209_9000.exe
133 http://yacy.net/release/yacy_v1.68_20140209_9000.dmg
134 http://localhost:8090/

Herhangi bir şey yazabilirsiniz. **4. seçenek ise diğer YaCy istemcilerinin de erişebilmesi için port ayarı**. Çok şart değil, port erişilebilir olursa hem performans açısından hem de diğer istemcilere indeks katkısı açısından biraz daha iyi olacaktır. Ayarlarınız tamamsa **Set Configuration** diyerek kaydedebilirsiniz. iptables'da port açmak isterseniz:

```
kame ~ $ iptables -I INPUT -p tcp --dport 8090 --syn -j ACCEPT
kame ~ $ iptables -I INPUT -p udp --dport 8090 -j ACCEPT
```

Arama



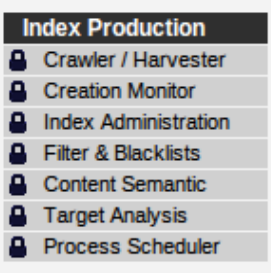
Görüldüğü üzere çok kapsamlı bir sonuç (*daha devam ediyordu fakat ben yarıda kestim*) elde edemedik. Bunun temel nedeni çok taze

bir konuyu aratmak istememdi, ayrıca daha çok robotlarla taramaya ve indekslemeye ihtiyacı olduğundandır. Diğer bir deyişle, YaCy'nin birçok istemciye ihtiyacı vardır. Fakat, bu arama YaCy'nin yetersiz olduğu fikri oluşturmasın. Şu ana kadar beni pek üzdüğünü söyleyemem. Sorgularıma verdiği yanıtlar hep yeterliydi.

Arama motoruna erişim

Evet. Herkes erişebilir. Bu ister YaCy istemcisi olsun, ister Internette arama moturunuzun açık adresini bilen olsun veya diğer arama portallarının örümcekleri olsun erişebilirler. Status sayfasında, sağ köşede bir kutu göreceksiniz. **Address** kısmına baktığınızda sunucu (*host*), açık adres (*public adress*) ve YaCy adreslerinizi (*yacy address*) görebilirsiniz. Açık adresinize herkes (*örümcekler dahil ve adresinizi dağıttığınız sürece*) erişebilir. Bu yüzden Account ayarlarında **Acces only with qualified account** seçeneği ile bir yönetici (*admin*) şifresi belirleyebilirsiniz. **Local robots.txt** bölümünden de örümceklerin neye erişemeyeceklerini de ayarlayabilirsiniz.

Indeks yapmak



Sol menüde **Index Production** alt menüsünü göreceksiniz. **Crawler/Harvester**'a tıkladığınızda açılan sayfa üzerinden indekslemek istediğiniz sayfanın linkini girerek bu işlemi gerçekleştirebilirsiniz.

Son Sözler

YaCy çok detaylı ve kapsamlı bir arama motorudur. Burada çok temel birkaç şeyden bahsettim. Genel anlamda dört temel özelliği vardır. Tarama (*crawl*), indeksleme, arama ve yönetici arayüzü ve veritabanı. Merkezi bir sunucusu yoktur, sansür, reklam, gözetim gibi durumlardan arındırılmıştır. Yüksek derecede gizlilik sağlar. Çeşitli sıkıntılara sahip olsa da kesinlikle desteklenmelidir. Son olarak, YaCy ne kadar çok istemci sahibi olursa o kadar çok etkin, güvenli, sansürsüz, reklamsız bir arama motoru olacaktır.

18. Tor Bir Öcü Mü?

> Gelen yorumlardan sonra bu yazıyı yazmak şart oldu. Tor bir öcü mü, anonimlik nedir bir bakalım.

Anonimlik nedir? **Anonimlik, özne setleri** (*anonimlik seti*) **içinde kimliğin saptanamaz olma durumuna denir**. Bu tanım ilk olarak 2000 yılında Pfitzmann ve Hansen tarafından yapılmış ve Anonim literatürü genelinde kabul edilmiştir. Pfitzmann-Hansen için anonimlik, bir öznenin başka özneler (*bir düşman, rakip, saldırgan*) tarafından farkedilmeden anonim olarak işlemine devam etmesidir. **Anonimliğin bu tanımı, ayrıca, düşmanların** (*rakiplerin, saldırganların*) **anonim özneler hakkında bilgi edinmeye çalışması olasılığını da ortaya çıkartmaktadır**. Anonimlik düzeyi ölçülebilir. Burada çok teknik detaya girmeyeceğim ama kısaca şunun iyi kavranması gerekli; Anonimlik kişisel tehlike modellerine dayanır. Kimsiniz, kimden gizleniyorsunuz? Neden ve ne tür bir risk alıyorsunuz? Bunun cevabını verecek olan da anonim olmak isteyen öznedir. Her öznenin farklı yöntemleri, aldığı farklı riskler vardır ve kısaca herbiri eşsizdir.

Anonimliğe kısa bir giriş yaptıktan sonra konuya Tor açısından bakalım. Tor, misyon olarak devam etmekte olan ifade özgürlüğü, çevrimiçi gizlilik hakları ve sansür alanlarında, teknoloji, müdafa, araştırma ve eğitim için küresel bir kaynak olmayı hedeflemektedir. Sizlere belirli bir düzey anonimlik sağlar, çeşitli riskler içerir (*mitm, dinleme vs*.) ve bunu da olabildiğince güvenli ve gereksiz işlem yükü bindirmeden yapar. Büyük medya organizasyonları tarafından (*özellikle*

yabancı) çok farklı şekillerde, özellikle çocuk pornosu, uyuşturucu, terörizme aracı gibi tanıtılmaktadır. Tor'u duyan kişiler genellikle bunu kullananlardan, konferanslardan, kendi websitesinden öğrenmediği ve genellikle bu medya organizasyonların yaptığı haberler ve yazdığı makalelerden öğrendiği için kafalarda çok farklı bir algı oluşmaktadır. Tor, bu "**kötü**" şeyler için yapılmış, yasa dışılığı savunan bir araç değildir. Fakat, bilinen şudur; evet birileri Tor'u kullanarak yasa dışı aktivitelerde bulunmaktadır.

Yasa dışı aktivitelere gelelim. Kötü bireyler, kötü bireylerdir. Tor olsun veya olmasın, zaten kötü bir şeyler yapmışlardır, yapıyorlardır veya yapacaklardır. Kaldı ki Tor'un sağlayacağı anonimlikten çok daha fazla seçeneğe sahiptirler. Bunun için büyük miktarlada para harcayabilirler, farklı ülkelerdeki bilgisayarları hackleyerek kötüye kullanabilirler vs. Fakat, parası olmayan, normal bir bireyin anonimlik için, ifade özgürlüğü için, sansürü aşabilmek için çok fazla bir alternatifi yoktur. Teoride suçluların Tor kullandığı söylenebilir, fakat daha fazla ve daha iyi seçeneklere sahiptirler. Tor'un olması veya olmaması onları kötü işler yapmaya devam etmekten alıkoymayacaktır.

Şimdi bir elimizde (*Suriye'de Tor ile rejime yakalanmadan ailesi ile iletişim kuran bir kız olayı var.*) ifade özgürlüğü kısıtlanmış, baskıcı bir ülkede, sansürden erişilemeyen sitelerde dünyaya sesini duyurmak isteyen bir birey var. Diğer elimizde de bu kötü bireylerden biri var. Soru şu; biz bu ikisini nasıl dengeleyeceğiz? Bu iki duruma nasıl bir değer vereceğiz? Bu durumları nasıl değerlendireceğiz? Baskıcı ülkede yaşayan bireyle, kötü işler yapan bireye nasıl bir değer atayacağız?

Bunların hangisinin daha önemli olduğuna nasıl karar vereceğiz? Cevabı kısaca şudur; bu seçimi yapmak kimseye düşmez. Baskıcı ülkede yaşayan kişinin elinden böyle bir seçeneği alırsanız kendini özgürce ifade edemeyecek, özgür bilgiye ulaşamayacak ve hatta öldürülebilecektir. Fakat kötü bireyin elinden Tor alınırsa, kötülük yapabilmek için farklı birçok yönteme başvuracaktır. Kaldı ki, normal bireyler, yani bizlerin Tor dışında çok fazla alternatifi yoktur.

Bununla birlikte, bir analiz için kurulan Exit Relay'e ait Tor trafiğinin %3'ünde "**kötü**" aktiviteye rastlanmıştır. Medyanın Tor'u nasıl öcü gibi gösterdiğine gelelim. BBC, Tor ve Silkroad ile nasıl uyuşturucu alınacağına dair bir makale yazıyor. İşin enteresan tarafı Tor geliştiricilerinin hiçbiri böyle bir şeyi savunmamasına rağmen makale Tor'un yasa dışı işler için kullanılan bir araç gibi göstermekte. Makalenin yorum kısmında ziyaretçilerden gelen "**artık sayenizde öldürülmeden uyuşturucu alacağım**" diyen teşekkür mesajları ile bir patlama yaşanıyor. Bu makalenin devamında gelen yeni BBC makalesinde ise uyuşturucu aldıklarını ve çok iyi olduğunu söylüyorlar. Burada amaç Tor'u bir öcü göstermenin ve yapmaya çalıştığını yıkmanın yanında daha fazla tıklama ve daha fazla gelir için makale yazmak da denilebilir.

Yazı ek olarak kısaca Tor kullanıcılarının bilmesi gereken basit bir terminolojiden bahsedeyim:

Web: The World Wide Web. Tarayıcı ile erişilebilen, Internetin parçasıdır.

Deep Web: Bilgisi hiçbir arama motoru tarafından kaydedilmemiştir.

Bu bilgi veritabanlarında tutulan veya yapılan istek sonrası oluşturulan sayfaları da kapsamaktadır.

Dark Web: Web'in herkerse açık Internet tarafından kolayca erişilemeyen, erişilmek için özel araçlara ihtiyaç duyulan kısmı. Tor ağı için Hidden Service, I2P ağı için eepsites.

Herkese Açık Internet: Herkesin kullanıma açık olan, devletler ve İSS'ler tarafından filtrelenen ve sansürlenen Internet.

Özel Ağ: Belirli bir amaç için oluşuturulan bilgisayar ağı.

Son olarak sıkça yapılan yanlış önerilerden bahsedeyim. Tor tarayıcısı nasıl geliyorsa, geldiği gibi kalmalı (*fingerprint ne kadar önemli kötü yollardan deneyimlemeyin*). Eklenti kurmayın, bir örnek isterseniz Adblock[135]. Reklamları engellerken Tor'un gerçek IP'yi sızdırdığı farkedilmiştir ve bu yüzden kurulması tavsiye edilmiyor. Bir diğeri Adobe Flash[136]. Bilgisayarınızda Adobe Flash eklentisi olsa dahi Tor tarayıcısında bunu aktif etmeyin. Son olarak Java. Tor tarayıcıda gördüğünüz üzere NoScript[137] eklentisi mevcut. Eğer güvendiğiniz bir site değilse scriptlere izin vermeyin.

135 https://addons.mozilla.org/en-US/firefox/addon/adblock-edge/?src=search
136 https://www.adobe.com/flashplatform/
137 https://addons.mozilla.org/en-US/firefox/addon/noscript/?src=cb-dl-users

19. DNS'nin Kökü

Gece itibariyle DNS'lerde bir sıkıntı olduğu söyleniyordu. Bana da bununla ilgili epey bir mesaj geldi. "**Şu İSS'yi kullanıyorum, şu DNS sunucusunu kullanıyorum fakat Internete bağlanamıyorum, zaman aşımı alıyorum**" diye gelen mesajlar sonrası kendim kontrol ettiğimde bir sıkıntı görememiştim. Fakat, Twitter'da konuyla ilgili tweet sayıları giderek artmaya başladı ve ardından da Chip Türkiye'nin "**Türkiye'de DNS'lerin de kökü kazınıyor!**" haberi geldi[138]. Sanırım, söylentilerdeki doğruluk payı giderek artmaya başladı diyebilirim.

Yazıyı yayımladıktan bir süre sonra tekrar taslak formuna aldım. DNS'lerin kökünün kazınmasından ziyade daha farklı bir şeylerin döndüğünü düşünüyordum. Sabah ise OpenDNS ve Google DNS sunucuları üzerinden yapılan sorguların her ne hikmetse Türk Telekom sunucularına yönlendiğini gördüm. Bunun birçok sebebi olabilir. DNS spoofing[139], DNS hijacking[140], arada bulunan bir transparan DNS proxysisi[141] ile sorguların açık DNS sunucularına ulaşmadan İSS'nin DNS sunucularına yönlendirilmesi gibi. Yaptığım basit bir analizde aldığım sonuç, yapılanı doğrular nitelikteydi:

```
kame ~ $ nslookup twitter.com 8.8.8.8
Server:    8.8.8.8
Address:   8.8.8.8#53
```

138 http://www.chip.com.tr/haber/turkiye-de-dns-lerin-de-koku-kaziniyor_46256.html
139 https://en.wikipedia.org/wiki/DNS_Spoofing
140 https://en.wikipedia.org/wiki/DNS_hijacking
141 https://network23.org/kame/2013/10/20/dns-leak-tehlikesi/

```
Non-authoritative answer:
Name    twitter.com
Address:  195.175.254.2

kame ~ $ nslookup twitter.com 208.67.222.222
Server:    208.67.222.222
Address:  208.67.222.222#53

Non-authoritative answer:
Name    twitter.com
Address:  195.175.254.2
```

Bir de engellenmemiş bir adresin çıktısına bakalım:

```
kame ~ $ nslookup duckduckgo.com 8.8.8.8
Server:    8.8.8.8
Address:  8.8.8.8#53

Non-authoritative answer:
Name    duckduckgo.com
Address:  176.34.131.233
Name    duckduckgo.com
Address:  46.51.197.88
Name    duckduckgo.com
Address:  46.51.197.89
```

Engellenmemiş adres için herhangi bir sıkıntı yok gibi durmakta. Şimdi bunu daha anlaşılır bir dille anlatalım. DNS (*domain name system*); türkçesi alan adı sistemi, Internet ağını oluşturan birimlerin IP

adreslerini akılda daha kolay tutulması için dönüştürülen adresleri (domain, www.duckduckgo.com gibi) ve iletişimi organize eden bir sistemdir. DNS sunucuları ise Internet adreslerinin IP karşlığının kayıtlı tutulduğu sunuculardır. Bir örnekle anlatmak gerekirse, www.duckduckgo.com adresini tarayıcınızdan girdiniz, bu Intenet adresindeki makine ile iletişim kurulabilmesi için DNS sunucusuna sorgunuz gitti, DNS sunucusu ise eğer bu isim karşılığındaki IP adresine sahipse, **50.18.192.250** dedi ve bu IP'ye sahip makineye yönlendirildiniz. Fakat, yukarındaki çıktıda Google DNS kullanıyorsanız ve tarayıcınızdan www.twitter.com yazdığınız anda sorgunuz gitmesi gereken Google DNS sunucuları yerine **195.175.254.2** adresine, yani Türk Telekom'a yönlendirildi.

Bu işin biraz da tekniğine bakalım. Bir İSS'siniz ve kötü niyetli bir DNS sunucusu yapmak istiyorsunuz. Bu DNS sunucunuzun IP'sini **195.175.254.2** olduğunu varsayalım. Diğer yanda, ülkenizde hizmet veren güvenilir Google gibi DNS sunucuları var. Siz bu sunucuları kendi kullanım amacınızla işleyişlerini manipüle edip yani gasp edip kendi kötü niyetli sunucunuza yönlendirdiniz (*route*). Ardından Google DNS kullanan biri Twitter'a girmek istedi. Sorgusunu gönderdi, hop bu sefer Google DNS yanıt verecekken kurduğunuz kötü niyetli DNS sunucusu yanıt verdi. Yani bunu yapabilmek için de adresi **twitter.com/195.175.254.2** olarak atadınız. twitter.com diyen 199.59.149.230'a erişmek yerine tanımlanmış olan **195.175.254.2** IP adresli makineye erişecektir. Bu makine ne yapabilir? Sizi burada bekletebilir, … kararla site erişime engellendi yazısı ile karşılayabilir, DNS sorgularını loglayabilir, sizlere gereksiz reklam sonuçları gösterebilir (*bunu yapan birçok İSS mevcu*t) vs.

Şu an bizim yaşadığım durum da; siz Google veya OpenDNS kullandığınız takdirde, sorgularınız Türk Telekom'un sunucusuna gidiyor ve burada bekletiliyorsunuz. Normalde bu DNS'ler ile erişmeniz gereken adrese de sahte DNS sunucusunda bekletildiğiniz için erişemiyorsunuz. Erişemediğiniz için de sadece yaptığınız sorgu biliniyor. Bu şekilde herhangi bir hesabın, kimin kullandığının bilinmesi mümkün olmaz. Fakat, bir spoofing yapılırsa o zaman işin rengi değişir. Spoofing'de de siz herhangi bir siteye bağlandığınızı zannedersiniz fakat IP/adres manipüle edildiği için hiç alakası olmayan, saldırganın bilgilerinizi çalacağı sahte bir yere ulaşırsınız. Böylece, örneğin Twitter'a giriş yaptığınızı sanarken sahte bir Twitter sitesi üzerinden tüm bilgileriniz alınabilir.

Şimdi bu yönlendirme ile ilgili bir diğer bir tespite gelelim. İlk başta ben Twitter ve Youtube'a girenleri mi tespit etmek istiyorlar, bu yüzden sadece bu ikisi mi yönlendirildi diye düşünmüştüm. Fakat sonradan rastgele, daha önce engellenmiş iki porno sitesi için tekrar nslookup yaptım. Sonuç:

```
kame ~ $ nslookup pornhub.com 8.8.8.8
Server:    8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name       pornhub.com
Address:   195.175.254.2
```

kame ~ $ nslookup xnxx.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name xnxx.com
Address: 195.175.254.2

Fakat, buna henüz gasp edilmemiş bir DNS sunucusu ile bakarsak:

kame ~ $ nslookup xnxx.com 77.88.8.8
Server: 77.88.8.8
Address: 77.88.8.8#53

Non-authoritative answer:
Name xnxx.com
Address: 141.0.174.37
Name xnxx.com
Address: 141.0.174.38
Name xnxx.com
Address: 141.0.174.35
Name xnxx.com
Address: 141.0.174.39
Name xnxx.com
Address: 141.0.174.34

Anlaşılan engelli tüm adresler Google DNS ve OpenDNS için aynı yere yönlendirilmiş durumda. İSS tarafından Yandex DNS'te[142] herhangi bir yönlendirme (*routing*) olmadığı için sonuç sorunsuz gözüküyor. Şimdilik, Google DNS ve OpenDNS kullanmamak, yaşanabilecek manipülasyonlardan ve spoofing gibi saldırılardan etkilenmeyi azaltacaktır. Kaldı ki Türk Telekom tarafından yapılan bu şeyin yasalara aykırı ve suç olduğu da söylenmektedir. Daha önce de DNS gaspı (hijacking) ile ilgili belirttiğim üzere İSS'ler bunu daha öncede yapabilmekte, olmayan sayfa sorgularında sizlere yanıt vermekte, bunu sahte DNS sunucuları ile gerçekleştirmekte, sorguları reklamların olduğu sitelere yönlendirmekteydiler.

Sonuç olarak, ortada ciddi bir sıkıntının olduğunu söylemek gerekli ve bu durum yakından takip edilmeli. Açıkçası gasp edilen 2 DNS sunucusunun engellenmemiş adreslerin sorgularına verecekleri yanıtlar da "kötü niyetli" birileri tarafından manipüle edilmeye açıktır. Şu anda dava hazırlıkları da yapılmakta. Yazıyı kafam çok karışmış bir şekilde yazdım. Hatam varsa şimdiden kusura bakmayın. Bilgilendirirseniz memnun olurum.

Bu konuyla ilgili olarak kısaca birkaç link vereyim (*siz de konuyla ilgili yazı linkleri verirseniz buraya eklerim*):

[1] http://www.turk-internet.com/portal/yazigoster.php?yaziid=46356

[2] https://eksisozluk.com/entry/41565793

142 http://dns.yandex.com/

Ekleme (03.04.2013): Twitter yasağı Anayasa Mahkemesi tarafından kaldırıldı ve sonunda TİB denilen kurum-cuk kademeli olarak engeli kaldırdıklarını duyurdu. Peki DNS yönlendirmesi bitti mi? Hemen VPN, Tor vs kullanmayı bırakıp Twitter'a girmek mantıklı mı? Yeni analizimize bakalım:

kame ~ $ nslookup twitter.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: twitter.com
Address: 199.16.156.70
Name: twitter.com
Address: 199.16.156.38
Name: twitter.com
Address: 199.16.156.198

Peki engeli henüz kaldırılmamış Youtube için bakalım:

kame ~ $ nslookup youtube.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name youtube.com
Address: 195.175.254.2

O da ne? DNS yönlendirmesi devam ediyor! Yani; VPN, Tor vs. kullanmaya GoogleDNS, OpenDNS gibi yönlendirilmiş DNS sunucuları kullanmamaya kaldığınız yerden devam ediyorsunuz.

20. Unbound

Bugün, Google[143] da Türk Telekom'un hukuki bir dayanak olmadan DNS sunucularını yönlendirdiğini ve Türkiye'deki Internet kullanıcılarının fişlendiğini belirten bir değerlendirme yaptı[144]. İletişim özgürlüğüne ve özel hayatın gizliliğine yapılmış sayısız ihlale bir yenisinin daha eklenmesinin yanında henüz TİB ve Türk Telekom'dan da konuyla ilişkili bir bilgi verilmedi. Türkiye'de Google ve Open DNS[145] sunucuları hukuka aykırı ve hiçbir dayanağı olmadan Türk Telekom'a yönlendiriledursun, bu durumu aşabilmek için çeşitli yöntemler de mevcuttur. Bunlardan biri GNU/Linux altında Unbound[146] kurarak kullanıcı kendini DNS önbellek zehirlemesinden ve sahte yönlendirmelerden koruyabilir. Ayrıca, özellikle DNS sorgusunda araya girilmediği ve yapılan sorguların bu şekilde elde edilmediği takdirde de gayet iyi bir yöntem olacaktır.

Unbound; önbelleğe sahip ve DNSSEC[147] doğrulaması yapan bir DNS çözümleyicisidir. Harici bir DNS sunucusuna ihtiyaç olmadan DNS çözümleme işlemini yerine getirir. İstenildiği takdirde harici DNS sunucusu da kullanılabilir. Bununla birlikte, DNSSEC ise Türkiye örneğindeki gibi kullancıyı ve uygulamayı manipüle edilen DNS verilerinden sahip olduğu dijital imza ile koruyan bir özelliktir. Biz ise örneğimizde DNSSEC doğrulaması yapan ve yerel bir DNS çözümleyici için Unbound kurup ayarlayacağız. İlk olarak, Türkiye'deki OpenDNS, Google DNS ve İSS'lerin kendi DNS sunucularının verdiği çıktıya

143 http://googleonlinesecurity.blogspot.ca/2014/03/googles-public-dns-intercepted-in-turkey.html
144 http://bianet.org/bianet/insan-haklari/154635-dns-ler-hukuksuz-sekilde-engelleniyor
145 http://opendns.com/
146 https://unbound.net/
147 https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

bakalım:

```
kame ~ $ nslookup twitter.com
Server:    192.168.1.100
Address:   192.168.1.100#53

Non-authoritative answer:
Name       twitter.com
Address:   195.175.254.2

kame ~ $ nslookup twitter.com 8.8.8.8
Server:    8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name       twitter.com
Address:   195.175.254.2

kame ~ $ nslookup twitter.com 208.67.222.222
Server:    208.67.222.222
Address:   208.67.222.222#53

Non-authoritative answer:
Name       twitter.com
Address:   195.175.254.2
```

Görüldüğü üzere iki DNS sunucusu ile İSS engelli sayfayı sahte bir DNS sunucusuna yönlendirilmekte ve kullanıcı sahte DNS

sunucusunda bekletilmektedir. Bu, Google'ın değerlendirmesi ve ayrıca daha önceden de bu konuya ilişkin yazılmış yazılar[148] da[149] doğrulamaktadır.

Kurulum

Şimdi, Debian ve türevi dağıtımlar için Unbound kuruluma geçecek olursak (*Windows için buradan[150] indirebilir ve yönergeler için el kitabına[151] bakabilirsiniz. Gayet basitçe anlatılmış*.):

kame ~ $ apt-get install unbound unbound-anchor

kame ~ $ sudo cp /etc/unbound/unbound.conf /etc/unbound/unbound.conf.save

kame ~ $ sudo wget -c ftp://FTP.INTERNIC.NET/domain/named.cache -O /etc/unbound/root.hints

kame ~ $ sudo cp /var/lib/unbound/root.key /etc/unbound/root.key

kame ~ $ sudo chown -R unbound:unbound /etc/unbound/root.key

kame ~ $ sudo nano /etc/unbound/unbound.conf

İçine:

```
server:
        auto-trust-anchor-file: "root.key"
        interface: 127.0.0.1
        interface: ::1
        root-hints: "root.hints"
```

148 http://www.turk-internet.com/portal/yazigoster.php?yaziid=46356
149 https://network23.org/kame/2014/03/29/dnsin-koku/
150 https://unbound.net/downloads/unbound_setup_1.4.22.exe
151 https://unbound.net/documentation/unbound-windows-manual-01.pdf

```
        num-threads: 2
        hide-identity: yes
        hide-version: yes
        msg-cache-size: 16m
        msg-cache-slabs: 8
        rrset-cache-size: 32m
        rrset-cache-slabs: 8
        infra-cache-numhosts: 20000
        infra-cache-slabs: 8
        key-cache-slabs: 8
        key-cache-size: 8m
        jostle-timeout: 250
        so-rcvbuf: 4m
        so-sndbuf: 4m
        harden-short-bufsize: yes
        harden-large-queries: yes
        harden-glue: yes
        harden-dnssec-stripped: yes
        harden-below-nxdomain: yes
        prefetch-key: yes
        prefetch: yes
        unwanted-reply-threshold: 10000000
        rrset-roundrobin: yes
        outgoing-range: 8192
        num-queries-per-thread: 4096
        do-udp: yes
        do-ip4: yes
        do-ip6: no
```

```
        do-tcp: yes
python:
remote-control:
forward-zone:
```

Kopyalayıp kaydedin. Ağ yöneticinizdeki DNS sunucuları ayarını 127.0.0.1 yapın ve Unbound servisini çalıştırın (*systemd ve openrc için iki örnek aşağıda*).

```
kame ~ $ systemctl enable unbound.service
kame ~ $ systemctl start unbound.service
kame ~ $ /etc/init.d/unbound start
```

Yukarıdaki ayarlar hemen hemen bütün dağıtımlarda çalışacaktır. Herhangi bir sıkıntı yaşayacağınızı düşünmüyorum. DNSSEC kontrolü yapalım:

```
kame ~ $ dig sigok.verteiltesysteme.net @127.0.0.1
; <<>> DiG 9.9.5 <<>> sigok.verteiltesysteme.net @127.0.0.1
;; global options: +cmd
;; Got answer:
;; HEADER opcode: QUERY, status: NOERROR, id: 5409
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sigok.verteiltesysteme.net. IN      A

;; ANSWER SECTION:
```

```
sigok.verteiltesysteme.net. 60      IN      A       134.91.78.139

;; AUTHORITY SECTION:
verteiltesysteme.net.       3600    IN      NS      ns1.verteiltesysteme.net.
verteiltesysteme.net.       3600    IN      NS      ns2.verteiltesysteme.net.

;; ADDITIONAL SECTION:
ns1.verteiltesysteme.net. 3600      IN      A       134.91.78.139
ns2.verteiltesysteme.net. 3600      IN      A       134.91.78.141

;; Query time: 1070 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Apr 01 11:49:29 2014
;; MSG SIZE  rcvd: 167
```

Bu şekilde A çıktısı alıyorsanız DNSSEC doğrulaması yapılmakta olduğunu söyleyebiliriz. Bununla birlikte, DNSSEC doğrulaması yapabileceğiniz siteler de mevcuttur:

- http://dnssec.vs.uni-due.de/
- http://test.dnssec-or-not.net

Şimdi, Unbound'un sorunsuz çalıştığını ve DNSSEC doğrulaması yapıldığını farzederek Twitter çıktımızı tekrar kontrol edelim:

```
kame ~ $ nslookup twitter.com 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
```

Name: twitter.com
Address: 199.59.148.82
Name: twitter.com
Address: 199.59.149.230
Name: twitter.com
Address: 199.59.149.198

Her şey yolunda gözüküyor. Yerel DNS çözümleyicimiz sayesinde İSS'nin yapmış olduğu yönlendirmeye takılmadan kullanabiliriz. Diğer yandan, adres/IP manipülasyonlarında da sahip olunan dijital imza ile kullanıcı korunabilecektir. Unbound, yerel DNS çözümleyici ve DNSSEC ile doğrulama gerçekleştirerek yaşanabilecek sıkıntıların engelleyebilmektedir. Türkiye'de Internetin gelmiş olduğu noktaya bakacak olursak herhangi bir sosyal medya üzerinde verilen DNS sunucularını kullanmak yerine Unbound iyi ve güvenli bir çözüm gibi durmaktadır. Açıkçası, Türk Telekom ve TİB'in bundan sonra ne tür bir yöntem ile Internet üzerinde kullanıcı takibi, sorgu denetimi yapabileceğini, SSL sertifikalarında mitm yapıp yapmayacağını, sahte sertifika üretip üretmeyeceğini de kestiremediğim için kesin bir şey söyleyemiyorum. Aceleci bir yapım olmadığı için bekleyip görmeyi tercih ediyorum.

21. Heartbleed

SSL/TSL[152] protokolü Internet üzerinde web sunucuları, tarayıcılar, e-posta, anlık mesajlaşma araçları ve VPN gibi uygulamaların şifreli bir şekilde haberleşmeleri için geliştirilmiştir. Temel amacı gizlilik ve güvenlik sağlamaktır. Açık ve gizli anahtara sahiptir. Açık anahtar ile şifrelenen veri gizli anahtar tarafından çözülür. Böylece iletilen verinin şifresinin doğru adreste ve doğru alıcı tarafından çözülmesi sağlanır. İşleyiş yapısına Wiki'den[153] (*Türkçe*) bakalabilirsiniz. Kısaca anlatacak olursak[154]:

- **Ali -> Selam -> Ayşe** diye bir mesaj yolladı. Bu mesaj desteklenen en yüksek TSL protokolü, rastgele bir sayı, doğrulama, şifreleme, mesaj doğrulama kodu (*MAC*) içeren şifreleme yöntemi ve bir sıkıştırma yöntemi ile yollandı.
- **Ayşe -> Selam -> Ali** diye cevap verdi. Bu cevap da Ali tarafından seçilen TSL protokolü, rastgele sayı, doğrulama, şifreleme, mesaj doğrulama kodu (*MAC*) içeren şifreleme yöntemi ve sıkıştırma yöntemine uygun olarak verildi.
- **Ayşe -> Sertifika -> Ali** mesajı yolladı. Bu mesaj şifreleme yöntemine uygun olarak şeçildi.
- **Ayşe -> SelamTamamlandı -> Ali** diye bir mesaj daha yolladı.
- **Ali -> AnahtarDeğişimi -> Ayşe** mesajı yolladı. Bu mesaj açık anahtarı (*PreMasterSecret veya hiçbir anahtar*) içermektedir. Bu değişimle artık üzerinden iletişim kurabilecekleri ortak bir sır

152 http://en.wikipedia.org/wiki/Secure_Sockets_Layer
153 https://tr.wikipedia.org/wiki/Secure_Sockets_Layer
154 http://en.wikipedia.org/wiki/Secure_Sockets_Layer#Basic_TLS_handshake

belirleyebilecekler.

- Ali ve Ayşe rastgele sayılar ve anahtar ile doğrulama ve şifrelemede kullanacakları ortak bir sır oluşturdular.
- **Ali -> ŞifrelemeYönteminiDeğiştir -> Ayşe** mesajı gönderdi. Bu mesaj "**Ayşe, bundan sonra sana göndereceğim her mesaj doğrulanacak ve şifrelenecek.**" anlamına gelmektedir.
- **Ali -> Bitti -> Ayşe** mesajı gönderdi. Bu mesaj oluşturulan sır ile doğrulanmış ve şifrelenmiştir.
- Ayşe Bitti mesajının şifresini çözmek isteyecektir. Eğer, oluşturdukları sıra uygun değilse el sıkışma gerçekleşmeyecektir.
- **Ayşe -> ŞifrelemeYönteminiDeğiştir -> Ali** mesajı gönderdi. Bu mesaj da "**Ali, bundan sonra sana göndereceğim her mesaj doğrulanacak ve şifrelenecek**" anlamına gelmektedir.
- **Ayşe -> Bitti -> Ali** mesajı gönderdi. Aynı şekilde oluşturulan sır ile doğrulandı ve şifrelendi.
- Ali de Bitti mesajının şifresini çözecektir.
- Son noktada, el sıkışma işlemi tamamlanmış olacaktır.

SSL/TSL'e kısa bir giriş yaptıktan sonra dün Heartbleed adıyla bir OpenSSL hatası keşfedildi. Heartbleed[155] adı ise TSL/DTSL'de olan heartbeat (RFC6520) uzantısındaki hatadan geliyor. Bu hata normal şartlar altında şifreli bir şekilde korunun verinin çalınmasına sebep olabilmektedir. Bununla birlikte, gizli anahtar ile şifreli verinin çözülmesi, kullanıcıların sahip oldukları kullanıcı adı ve şifre gibi

155 http://heartbleed.com/

içeriklerin elde edilmesi, iletişimin dinlenebilmesi, verilerin servis veya kullanıcılardan hiçbir şekilde farkında olmadan çalınmasına olanak sağlamaktadır. Diğer yandan, yapılabilecek herhangi bir saldırının kolaylığı ve iz bırakmaması kullanıcıları büyük bir risk altına sokmaktadır. Yukarıdaki işleyiş örneğine de bakacak olursanız Ali ile Ayşe arasında geçen şifreli iletişim bu hata yüzünden saldırganların iletişimde kullanılan şifrelere sahip olmalarına ve mesaj içeriğini çok kolay bir şekilde elde edebilmelerine neden olmaktadır.

Nelerin sızmış olabileceğine dair olarak dört kategori oluşturulmuş. Bunlar; birinci anahtarlar, ikincil anahtarlar, şifreli veriler ve hafıza içerikleridir. Kısaca özetlersek; birincil anahtarlar şifreleme için kullanılan açık ve gizli anahtarları içermektedir. Saldırganın servisler tarafından şifrelenen trafiğin arasına girilebileceği, şifreyi çözebileceği, özellikle geçmiş trafiğin hatanın yamalansa bile şifresinin çözülebileceğidir. İkincil anahtarlar, servislerde kullanılan kullanıcı adı ve parola gibi kullanıcı içerikleridir. Şifreli veriler, servislerde tutulan verilerdir. Bunlar iletişime konu olan veriler, e-postalar, belgeler veya şifrelemeye konu olan herhangi bir içerik olabilmektedir. Hafıza içerikleri de hafıza adreslerinde tutulan teknik detaylar olabildiği gibi çeşitli saldırılara karşı alınan güvenlik önemleri de olabilmektedir.

Ben de etkileniyor muyum?

Malesef etkileniyorsunuz. OpenSSL Internet üzerindeki trafiği şifrelemek üzere en çok kullanılan açık kaynak şifreleme kütüphanesi olduğu için en çok kullanılan sosyal medya siteleri, kurduğunuz SSL içerikli bir uygulama, ağ uygulamaları, hatta devlet siteleri bile gizlilik ve işlemleri (*trafik, giriş vs.)* korumak adına bu protokolü kullandığı için

etkilenmektedir. Bu yüzden sizler de doğrudan veya dolaylı olarak etkilenmektesiniz. Ayrıca, ilk keşfedenlerin bu hatayı bulanlar olmadığını da unutmamalısınız. Hatayı duyuran Codenomicon[156] ve Google'dan Neel Mehta[157] yaptıkları test saldırılarında durumun çok ciddi olduğunu ve bu açığın çoktan kullanılmış olabileceğini belirtmektedirler.

Hangi OpenSSL sürümleri etkilenmekte?

- OpenSSL 1.0.1 ve 1.0.1f etkilenmekte,
- OpenSSL 1.0.1g etkilenmiyor,
- OpenSSL 1.0.0 etkilenmiyor,
- OpenSSL 0.9.8 etkilenmiyor.

Hangi GNU/Linux dağıtımları etkilenmekte?

- Debian Wheezy, (*OpenSSL 1.0.1e-2+deb7u4*) etkilenmekte,
- Ubuntu 12.04.4 LTS, (*OpenSSL 1.0.1-4ubuntu5.11*) etkilenmekte,
- CentOS 6.5, (*OpenSSL 1.0.1e-15*) etkilenmekte,
- Fedora 18, (*OpenSSL 1.0.1e-4*) etkilenmekte,
- OpenBSD 5.3 (*OpenSSL 1.0.1c 10 Mayıs 2012) ve 5.4 (OpenSSL 1.0.1c 10 Mayıs 2012*) etkilenmekte,
- FreeBSD 8.4 (*OpenSSL 1.0.1e*) ve 9.1 (*OpenSSL 1.0.1c*) etkilenmekte,
- NetBSD 5.0.2 (*OpenSSL 1.0.1e*) etkilenmekte,

156 http://www.codenomicon.com/
157 https://google.com/

- OpenSUSE 12.2 (*OpenSSL 1.0.1c*) etkilenmekte.

Ne yapmalı?

Servis tarafını ilgilendiren duruma biz herhangi bir şey yapamıyoruz. Sadece, onların SSL sertifikalarını güncellemelerini bekleyeceğiz. Ardından, bir önlem olarak kullandığımız parolalarımızı değiştireceğiz. Bununla birlikte, bizi ilgilendiren tarafta ise ilk olarak dağıtımlarınızda kurulu olan OpenSSL paketinin sürümünü kontrol edin. Kontrol ettiğimde bende yüklü olan **1.0.1f** olan sürümü **1.0.1g**'ye düşürüldü. Eğer, bu açıktan etkilenen bir sürüme sahipseniz ilk iş olarak etkilenmeyen sürümlere geçin. Muhtemelen, bir güncelleme çıkmıştır.

21. Rapor – I

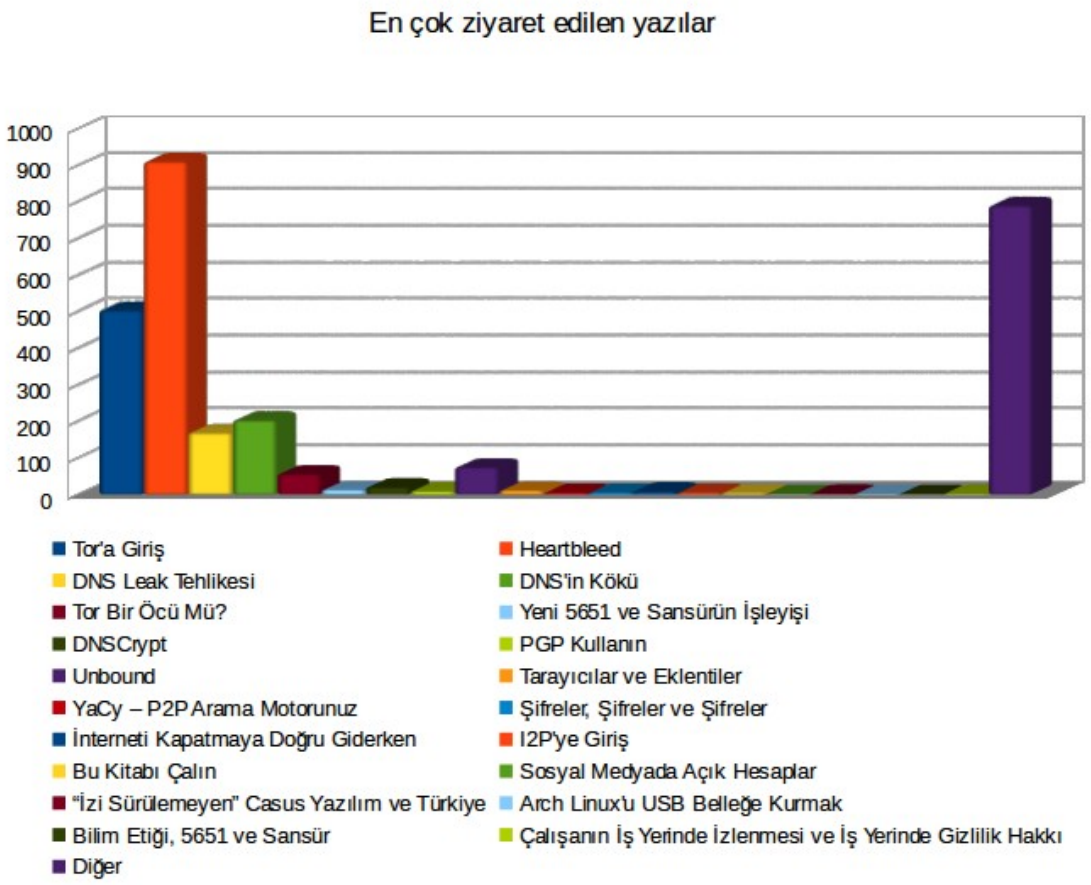
Kame'yi açtığım Ağustos 2013'ten Nisan 2014'e kadar kaç ziyaretçi geliyor, ne kadar okunuyor veya hangi yazılara ilgi var hiçbir fikrim yoktu. Network23, Mart ayının sonunda Piwik istatistiklerini aktif ettikten sonra blog ziyaretçilerinin de sayısal ve bazı tanımlayıcı bilgilerini (*Kesinlikle IP ve ülke bilgileri yok. Sadece tarayıcı, ekran çözünürlüğü, en çok ziyaret edilen yazılar, anahtar kelimeler, yönlendiren websiteler vb.*) görebilme fırsatım oldu. Açıkçası, bu istatistikler pek önemsediğim veya beni teşvik edici şeyler değil. Hatta hiç aktif edilmemesini de isterdim. Malesef, bu tarz hizmet aldığınız yerlerin işleyişilerine karışamadığınız için size sunulanı kullanmak durumunda kalıyorsunuz.

Durum böyle olunca ben de bundan sonra sizlere Kame'ye ait istatistikleri (*15 günlük*) şeffaflık amacıyla Türkiye'de ve Dünya'da yaşanan güncel konuları da dikkate alarak paylaşacağım. Şimdilik, bu istatistikleri 4 bölüme ayırdım. Bu bölümler sırasıyla:

1. En çok ziyaret edilen yazılar,
2. Ziyaretçilerin işletim sistemleri,
3. Ziyaretçilerin kullandıkları tarayıcılar,
4. Anahtar kelimeler.

Ziyaret edilen yazının okunup okunmadığını bilemeyeceğim için en okunan değil, en çok ziyaret edilen yazılar olarak belirttim. Ayrıca, iPhone, iPad ve iPod'un bir işletim sistemi olmadığını da biliyorum

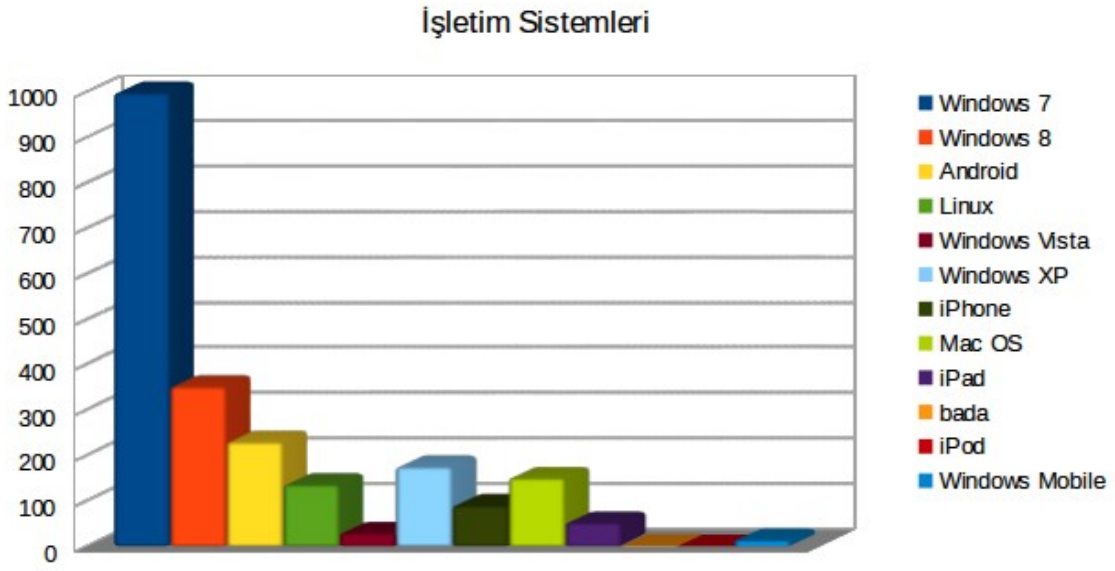
(*gülücük*). Analize başlamadan önce ilk olarak Kame'nin tanımını yapayım. Böylece, analiz daha anlamlı ve kapsamı daha belirgin hale gelecektir. Kame; I**nternet kullanıcılarını sansür, gözetim, erişim engelleri vb. konularda hem felsefi hem de teknik olarak bilgilendiren, anonimlik araçlarını anlatırken bu araçları kullanıma iten temel nedenleri sayan ve daha sonra kullanıma ait bilgi veren, bu çerçevede siyasi eleştiriler de getiren, inanç, dil, etnik kimlik, görüş gibi ayrımlar yapmadan herkesin hakkını savunmayı amaçlayan bir blogdur**. Bu tanım kapsam olarak genişletilebilir, eksik gördüğünüzü düşündüğünüz bir şey olursa lütfen belirtin.



Nisan ayı itibariyle en çok ziyaret edilen yazı, gündemin de sıcak konusu olan Heartbleed[158] olmuştur. Düzenli ziyaret edilen yazılar ise Tor'a Giriş[159], DNS Leak Tehlikesi[160] ve DNS'in Kökü[161] olarak durmaktadır. Ayrıca, geçmiş yazılardan PGP Kullanın[162], Sosyal Medyada Açık Hesaplar[163] ve Şifreler, Şifreler ve Şifreler[164] de az da olsa ilgi görmektedir. Diğer sütunu Piwik'te ziyaret alan fakat sıralamaya giremeyen yazıları ifade etmektedir. Aslında bu kısmın içeriğinin bilinmesi de iyi olabilirmişti. Toplama bakıldığında öne çıkan yazıları hem benim görmem hem de burada daha açık bir şekilde ifade etmeme olanak sağlayabilirdi.

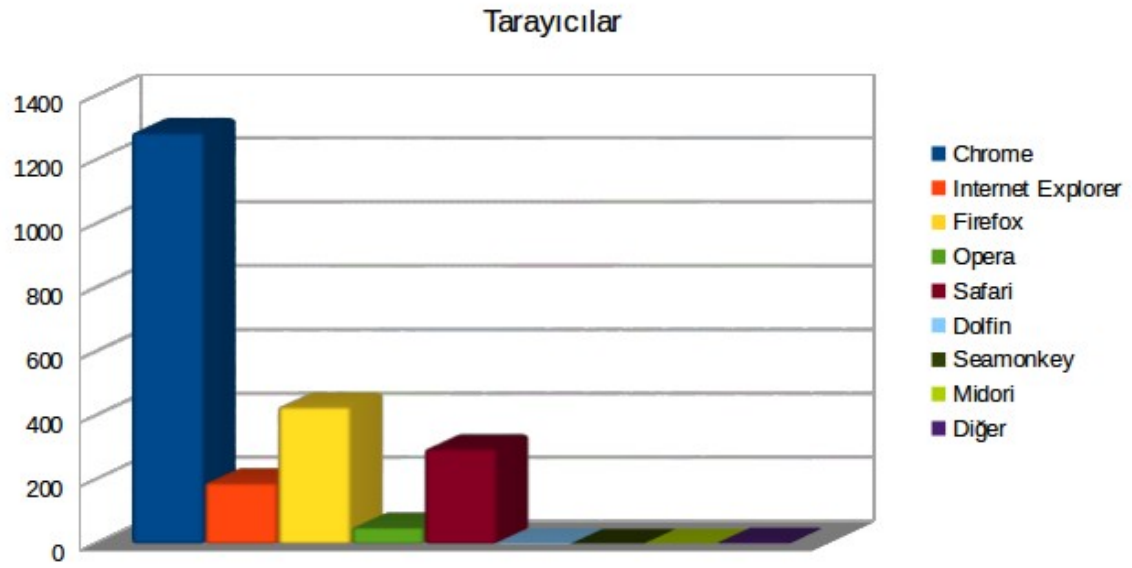
Türkiye'de yaşanan gelişmeleri de dikkate alacak olursak, sansürü ve engeli aşmak için Tor'a olan ilgi Twitter yasağının kalkmasından azalmış gibi gözükmekte fakat hâlâ Internet kullanıcılarının yoğun ilgisini çekmektedir. Bunu, yazının hergün ortalama 30 tekil ziyaretçi alması da göstermektedir. Öte yandan, I2P'ye olan ilginin düşük olması da benim açımdan düşündürücüdür. Buna yorum olarak, kullanıcıların kurulum ve kullanım kolaylığını tercih ettikleri ve bu yüzden de Tor'u tercih ettiklerini getirebilirim. Beni düşündüren bir diğer nokta da kullanıcıların sansür yazılarından çok sansürü aşmaya yönelmeleridir. Bu analiz çok kısa bir dönemi kapsasa da sadece anonimlik araçlarının okunuyor olması, sansürün nedenlerini gözardı ediyor ve kısa vadeli çözümlere yöneliyor oluşumuzdan kaynaklandığına -*kesin nedeni olmamakla birlikte*- işaret etmektedir.

158 https://network23.org/kame/2014/04/08/heartbleed/
159 https://network23.org/kame/2013/10/14/tora-giris/
160 https://network23.org/kame/2013/10/20/dns-leak-tehlikesi/
161 https://network23.org/kame/2014/03/29/dnsin-koku/
162 https://network23.org/kame/2013/08/28/pgp-kullanin/
163 https://network23.org/kame/2013/08/19/sosyal-medyada-acik-hesaplar/
164 https://network23.org/kame/2013/10/29/sifreler-sifreler-ve-sifreler/



İşletim sistemlerine ait istatistikleri inceleyek olursak, Windows'un beklediğim gibi bir yoğunluğu gözükmektedir. Anladığım kadarıyla Windows kullanıcıları XP'den sonra 7'ye kaymış gibi durmaktadırlar. Benim açımdan sevindirici bir gelişme olarak Android'in 3. sırada olmasıdır. GNU/Linux kullanıcılarının tedavülden kalkan Windows XP'nin ve Mac OS'un da gerisinde kalması biraz üzdü diyebilirim. Özellikle NSA ve Microsoft işbirliğinin, NSA slaytları ve Snowden'in önemle vurguladığı noktalara rağmen, Türkiye açısından kullanıcıların ilk olarak Türkiye'yi dikkate alıp küresel gözetim ve izlemenin bu anlamda *-kesin nedeni olmamakla birlikte-* gözardı edilebilir olduğu şeklinde gözükmesidir. Bu sakın şu anlama da gelmesin; Türkiye'de (*veya her yerde*) kullanıcılar sadece GNU/Linux kullansın, başka bir şey kullanmasın. Ben sadece kendi kullandığım ve deneyim sahibi olduğum şeyleri önerdiğim için mümkünse Windows kullanılmamasını ve özellikle Windows XP kullanıcılarının karar vermek

amaçlı GNU/Linux denemelerini öneriyorum. Ayrıca, sizleri Windows'a bağlayan çok belirgin bir şey yoksa (*örneğin 3D yazılımlar vs.)* ufak ufak sanal makinelerde GNU/Linux kurulum ve denemeleri de yapıp göç için hazırlığa başlayabilirsiniz.



Tarayıcıları inceleyecek olursak, Chrome'un bu kadar yüksek kullanım oranına sahip olduğunu pek düşünmezdim. Başka bir şekilde ifade edecek olursam, Chrome ile Firefox arasındaki farkın en azından bu kadar fazla olmamasını beklerdim. Açıkça söylebilirim ki, hem Windows hem de GNU/Linux kullanıcıları olsun, genel olarak varsayılan tarayıcılar yerine Chrome'u tercih etmektedirler. Çok kısa süreli de olsa kullandığım Opera'nın ise anladığım kadarıyla kullanıcılarını Chrome'a kaptırmış gibi durmaktadır. Zorlama bir yorum olabilir; Firefox ve Chrome kullanıcıları yeni bir tarayıcı arayışında bu ikisinden birini tercih ederken diğerlerini tercih etmemekte, fakat diğer tarayıcıları kullananlar ise yoğunluk Chrome'da olmakla birlikte Firefox'a

kaymaktadırlar. Yorumlardan sonra şunu da eklemek istiyorum; Chrome’daki kullanıcı artışının erişim engellerini aşmak için kullanılan ZenMate gibi eklentilere yönelimin artırması da olabileceği dikkate alınmalıdır. Aynı durumun Firefox için geçerli olmamasının sebepleri konusunda emin olmadığımı da belirtmeliyim.

Son olarak, arama motorlarında aratılan kelimeler üzerinden Kame’ye erişenlere bakacak olursak:

- ayar yapılmadan izlenebilir pornolar
- sansürü etkilemeyen porno siteleri
- dnsyle porno sitelerine yakalanmadan girebilir miyiz
- telefondan porno hangi siteden bakılır
- porno vide aramak hangi programlar
- reklamsız sansürsüz iğrenç pornolar
- internetten porn izlerken jandarma engeli
- yasak olduğunu bilmeyerek porno izlemek suç mu

Bu liste epey gidiyordu ama ben 8 tanesini paylaştım. Çoğunluk, sizlerinden de tahmin edeceği gibi “porno” üzerine yapılan aramaları içermektedir. Hatta aklınıza bile gelmeyecek içinde porno geçen sorgular var. Benim bu konudaki görüşüm; Kame sansür, gözetim ve erişim engelleri konusunda bilgilendirici engelleri aşmak konusunda yön gösterici bir site olarak düşünülürse, kullanıcılar porno izlemek istediklerinde erişim engelleri ile karşılaştıklarından dolayı bu engelleri

aşmak için çözüm arayışına girmekte, fakat genel anlamda sansürü önemsememektedirler.

Sonuca gelecek olursak, Kame'nin yapılan tanımı kapsamında; Türkiye'de Internet kullanıcıları sansür, gözetim ve engelleri aşmak için kısa vadeli arayışlar içine girerlerken sansürün yapısı, işleyişi ve olumsuz etkileriyle çok fazla ilgilenmiyor gözükmektedirler. Ek olarak, porno; Türkiye ölçeğinde sansürü aşmak için kullanılan araçların araştırılmasında büyük bir katalizör olarak durmaktadır. Diğer taraftan, yaşanan gelişmelere rağmen Windows kullanım oranlarının yüksek, açık kaynak ve özgür yazılımlara olan ilginin hâlâ çok az olması küresel gözetimin ikinci plana itildiğine bir işaret olarak sunulabilir. Son olarak, bu analiz ve istatistikler kısa bir dönemi kapsasa da bu sonuçların uzun vadede beklentinin daha fazla aksi yönünde gerçekleşebileceği de unutulmamalıdır.

Not: Bu yazıyı okuyan size sevgili ziyaretçilerden bir isteğim olacak. Eğer, GNU/Linux'a göç planları yapıyor fakat nereden başlayağacağınızı bilmiyor, hangi dağıtım, kurulum ve sonrası için basit bir anlatımla bu blogda yazılan yazılar gibi bir rehber istiyorsanız lütfen yorumu kullanarak bildirin. Bununla ilgili Şubat ayında da bu blogun takipçilerinden biriyle de iletişimim olmuştu. Yorumlarda en çok geçen dağıtımı temel alacağım. Bu yüzden özellikle isim belirtirseniz memnun olurum.

Ekleme (09.05.2014): Sizlerden gelen yorumlarda dağıtım olarak Lubuntu çoğunlukta olduğu için Lubuntu'yu temel alacağım.

22. Kriptografiye Giriş – I

> Kriptografi çok geniş ve hem tarihsel hem de teknik anlatım açısından uzun bir konu olduğu için giriş kısmını iki parçadan oluşturdum. Bu ilk kısımda eski dönemlerde neler yapıldığı ve nasıl yapıldığı basit örneklerle anlatıldı.

Yüzyıllardır krallar, kraliçeler, generaller ülkelerini ve ordularını yönetebilmek, toprak bütünlüklerini koruyabilmek için etkili ve güvenli bir iletişimden destek aldılar. Aynı zamanda, mesaj içeriklerinin düşmanların eline geçmesi ile gizli bilgileri ortaya çıkartabileceği, ülke çıkarlarını tehlikeye sokabileceğini ve bunların yaratacağı tehlikenin de farkındaydılar. Bu yüzden mesaj içeriğini sadece mesajı alanın okuyabilmesi için kodlar ve şifreleme yöntemleri geliştirildi. Gizliliğe olan tutku, ulusların iletişimin güvenliğini sağlamak içn en iyi şifreleme yöntemlerini oluşturmak ve uygulamak için kod üreten bölümler oluşturmalarına neden oldu. Bu aynı zamanda da düşmanların şifreleri kırabilmek için uğraşmalarını ve gizli içeriği çalabilmelerini de sağladı[165].

Kriptografi, eski Yunanca'dan (k*ryptos ve graphien*) gelmektedir. Genel olarak, birinin mesaj içeriği sade bir şekilde gizlemeye çalışması pratiği anlamına gelen "**gizli yazı**"'dır. Temel anlamda, kriptografi; orjinal mesajı dönüştüren bir formül olan anahtara ya da gizlice kodlanmış mesaja denir. Bu kodlamının yapılması sürecine şifreleme, tersi işlemine de şifre çözme denmektedir[166]. Mesajın bir anahtar ile şifreli koda dönüştürülmesi çok basit olabilir, fakat bu konuda birçok

165 Singh, S. (2002). The Code Book: How to make it, break it, hack it, crack it. New York: Delacore Press
166 Curley, R. (2013). Cryptography: Cracking Codes. New York: Britannica Educational Publishing

teknik mevcuttur. Ayrıca, bu dönüşüm işlemi daha karmaşık ve şifreli kodun çözülmesi ise daha zor olabilmektedir. Kriptografi'ye kısa bir giriş açısından bu yazıda ise sadece belirli bazı tarihsel olaylara bakacağız.

Romalı ünlü bir filozof ve devlet adamı olan Cicero'ya[167] göre gizli yazışmalar Herodot[168] dönemine kadar uzanmaktadır. Herodot yazılarında İ.Ö. 5.yy'da Yunan şehirlerininin özgürlüğünü ve bağımsızlığını tehdit eden Pers saldırılarından bahsetmektedir. Bu konudaki yazılarından dikkati çeken bir şey de gizli yazışmaların Yunan şehirlerini depotik Pers imparatoru Xerxes'ten[169] kurtardığıdır. Xerxes, imparatorluğu için yeni başkent olarak Persepolis'i[170] inşaa etmeye başladığında Atina ve Sparta hariç tüm imparatorluktan ve komşu devletlerden hediyeler almıştı. Bu durum ise Yunanistan ile Pers İmparatorluğu arasındaki düşmanlığı bir krize çevirmişti. Kendini aşağılanmış hisseden Xerxes, "**Pers İmparatorluğu'nun sınırlarını Tanrı'nın sahip olduğu gökyüzü, güneşin üzerine bakamayacağı uzunlukta topraklar kadar olmalı.**" diyerek ordusunu toplamaya başladı.

İlerleyen 5 yıl içerisinde Xerxes tarihin gördüğü en büyük savaş gücünü gizlice oluşturdu ve İ.Ö. 480'de süpriz saldırı için hazırdı. Bununla birlikte, aynı zamanda Yunanistan'dan sürülmüş ve Susa[171] adında bir Pers şehrinde yaşayan Demaratus[172], Pers ordusunun

167 http://en.wikipedia.org/wiki/Cicero
168 http://en.wikipedia.org/wiki/Herodot
169 http://en.wikipedia.org/wiki/Xerxes_I_of_Persia
170 http://en.wikipedia.org/wiki/Persepolis
171 http://en.wikipedia.org/wiki/Susa
172 http://en.wikipedia.org/wiki/Demaratus

hazırlıklarına şahit olmuştu. Sürülmesine rağmen hala Yunanistan'a bağlılık duyan Demaratus, Sparta'yı Xerxes'in işgal planı hakında uyarmıştı. Bunu ise ağaç tabletlerin içine mesajlarını kazıyıp üzerine ise balmumu ile kapatatarak yapmış, böylece kontrolden geçen ağaç tabletler boş gibi gözükmüşlerdi. Demaratus'un bu gizli iletişim stratejisi basitçe mesajı gizlemeye dayanmaktadır. Ayrıca, mesajı gizlemeye benzer olarak aynı dönemlerde Histiaeus[173], Miletus'u Pers imparatoruna karşı ayaklandırmak için elçisinin başını kazıyıp mesajı kafasına kazımış ve elçi Miletus'a ulaşana kadar saçları uzadığı için mesaj gizli kalabilmişti[174].

Mesajın içeriğinin saklanarak yapılan gizli iletişime Yunanca'dan gelen **steganografi** denmektedir. Önemli bir nokta olarak bu bir "**şifreleme**" değildir. Steganografi'ye ait birçok örnek bulabilmek mümkündür. Eski Çinliler kaliteli ipeğe yazdıklarını balmumu ile top haline getirip elçiye yuttururlarmış. Kurt sütü olarak anılan tithymalus[175] bitkisinden elde edilen sütü Romalı Gaius Plinius Secundus[176], görünmez mürekkep olarak kullanmıştır. Özelliği ise kuruduktan sonra transparanlaşan yazılar, yazıldığı yerin belirli bir oranda ısıtılması ile kahverengiye dönüşmektedir. Karbon açısından zengin birçok organik sıvının da buna benzer özellikler taşıdığı bilinmektedir.

Kriptografi'nin kendisi iki kola bölünebilir; yerini değiştirme ve yerine koyma. Yerini değiştirmede mesaja ait harfler yeniden

173 http://en.wikipedia.org/wiki/Histiaeus
174 Singh, S. (2002). The Code Book: How to make it, break it, hack it, crack it. New York: Delacore Press
175 http://en.wikipedia.org/wiki/Tithymalus
176 http://en.wikipedia.org/wiki/Pliny_the_Elder

düzenlenir, harflerin yerinin değiştirilmesine anagram da denilmektedir. Bu yöntem, özellikle tek bir kelime için göreceli olarak güvensizdir, çünkü sadece birkaç harfin yeri değiştirilerek yeni bir kelime oluşturulacaktır. Örneğin; kame, kmea, kmae, kema… Diğer yandan, harf sayısı arttıkça oluşuturulabilecek yeni kelime sayısı da artmaktadır. Örneğin, 10 harften oluşan bir kelime veya cümle sayısı 10! gibi büyük bir sayıya ulaşmaktadır. Harflerin rastgele yerine konulması göreceli olarak daha yüksek bir güvenlik sağlamaktadır. Fakat, herhangi bir yöntem veya neden olmadan oluşturulan yeni kelimeler alıcı için de çözülmesi imkânsız hale gelebilmektedir. Bu yüzden yerini değiştirme belirli bir sistemi takip etmektedir. Buna bir örnek olarak **ray dizilimi** verilebilir.

BU GİZLİ BİR MESAJDIR

B G Z İ İ M S J I

U İ L B R E A D R

BGZİİMSJIUİLBREADR

İ.Ö. 4.yy’da da Sparta’da **skytale** adı verilen çokgen şeklinde bir sopa da yerini değiştirmeye örnek olarak verilebilir. Bu çokgen sopanın her bir yüzeyine yazılan yazılar çevrilerek okunur. Örneğin altıgen bir sopa:

```
    |   |   |   |   |   |   |
    | K | A | M | E | G |   |
 __| İ | Z | L | İ | K |__ |
|  | V | E | G | Ü | V |
|  | E | N| L | İ | K |
|  |   |   |   |   |   |
```

KAMEG, İZLİLİK, VEGÜV, ENLİK = KAME GİZLİLİK VE GÜVENLİK

Yerini değiştirmenin alternatifi ise yerine koymadır. Yerine koymaya ait şifrelemenin ilk olarak Kâma-sûtra'da[177], İ.S. 4.yy'da Brahman öğrencisi Vatsyayana[178] tarafından kadınlara ahçılık, masaj, parfüm hazırlama, giyim gibi şeyleri öğretmek için oluşturulan 64 Kâma-sûtra resimden oluşmaktadır. Bu resimlere marangozluk, satranç ve büyü gibi resimler de dahildir. 45 numaralı resim mlecchita-vikalpa adında, gizli yazışma sanatı olan ve kadınlara gizli ilişkilerini saklamayı tavsiye eden bir resimdir. Temel olarak yerine koymaya dayanır. Örneğin:

```
A E M K
|  |  |  |
Q P W O
```

Bu yöntemle biri sizlere "**KAME**" için "**OQWO**" yazması gerekecektir. Bu yöndemin ilk kullanılması Julius Caesar'ın[179] Galya

177 http://en.wikipedia.org/wiki/Kama_Sutra
178 http://en.wikipedia.org/wiki/Vātsyāyana
179 http://en.wikipedia.org/wiki/Julius_Caesar

Savaşları[180] dönemine kadar gitmektedir. Tarihte kriptografi ile ilgili önemli olayardan biri de 7 Şubat 1587 yılında İskoç Kraliçesi Mary'nin[181] idamıdır. İdam kararının gerekçesi tacı kendine alabilmek için Kraliçe Elizabeth'e[182] suikâst girişimi ile vatana ihanettir. Kraliçe Elizabeth'in baş sekreteri olan Francis Walsingham[183], diğer komplocuları yakalamış, idam etmiş ve komplonun kalbindeki ismin Kraliçe Mary olduğunu kanıtlamak istemişti. Bu yüzden de Kraliçe Elizabeth'e Kraliçe Mary'nin suçlu olduğuna inandırması gerekmekteydi. Kraliçe Mary'nin direkt idam edilmemesinin sebesi ise eğer bir kraliçe idam edilirse isyancılar da cesaret bularak bir başka kraliçeyi öldürmek isteyebileceklerdi. Diğer yandan, Kraliçe Elizabeth ve Kraliçe Mary kuzenlerdi. Komplocular İngiliz Katolikleri'ydiler ve Protestan olan Kraliçe Elizabeth'i Katolik olan Kraliçe Mary ile değiştirmek istiyorlardı. Kraliçe Mary ile komplocular arasındaki gizli yazışmalar belirli bir şifreleme ile olmaktaydı ve Walsingham bu mektupları yakalasa bile kelimelerin ne anlama geldiği bilemeyecek algısı vardı. Fakat, Walsingham sadece baş sekreter değil ayrıca İngiltere gizli servisinin başındaki isimdi. Walshingman'ın Kraliçe Mary'e ait olan ve tarihte **kanlı mektuplar** olarak anılan gizli mektupları ele geçirmesi ile ülkenin şifre çözmesiyle ün yapan ismi Thomas Phelippes[184], bunları çözerek Kraliçe Mary'nin idam edilmesi önündeki engel de ortadan kaldırmıştır.

180 http://en.wikipedia.org/wiki/Gallic_Wars
181 http://en.wikipedia.org/wiki/Mary,_Queen_of_Scots
182 http://en.wikipedia.org/wiki/Elizabeth_I_of_England
183 http://en.wikipedia.org/wiki/Sir_Francis_Walsingham
184 http://en.wikipedia.org/wiki/Thomas_Phelippes

İslâm dünyasında ise tıp, astronomi, matematik, etimoloji ve müzk alanlarında toplam 290 kitap yayınlayan Al-Kindi'nin[185] şifre çözme üzerine olan "**Şifrelenmiş Mesajların Şifresini Çözme Üzerine Bir El Yazısı**" adlı 850'lerde yazdığı kriptoanaliz üzerine eseri, 1987 yılında İstanbul Osmanlı Arşivi'nde keşfedilmiştir. Özellikle istatistik ve Arapça üzerine yoğunlaşmış olsa da Al-Kindi'nin devrimsel keşfi "**Şifrelenmiş bir mesajı çözmenin bir yolu; eğer biz yazının dilini biliyorsak o dile ait bir sayfa dolusu yazı bulur ve her harfin görülme sıklığına bakarız. En çok tekrarlanan harfin ilk harf şeklinde bütün farklı harfleri ve sırasını bulana kadar sıraya dizeriz. Daha sonra çözmek istediğimiz şifreli mesaja bakar ve ayrıca sembolleri sınıflandırırız. En çok tekrarlanan sembol daha önce oluşturduğumuz sıradan ilk harf olacak şekilde bütün sembolleri tamamlayana ve şifreli mesajı çözene kadar devam ederiz.**" demektedir[186].

800 -1200 yılları arasında Araplar entelektüel ilerlemenin keyfini sürerken ve Al-Kindi'nin kriptoanaliz üzerine eserine rağmen, Avrupa basit kriptografi ile uğraşmakta idi. Fakat, 15.yy'dan sonra Avrupa'da Rönesans ile kriptografi de büyüyen bir endüstri haline dönüştü. Rönesans'ın kalbi olduğu için özellikle İtalya'da her şehirde şifreleme ofisleri kurulmuştu ve her büyük elçi bir şifreleme uzmanına sahipmişti. Aynı zamanda şifreleme bir diplomasi aracı haline gelmiş ve kriptoanaliz bilimi de Batı'ya entegre olmaya başlamıştı. Bu dönemlerde kriptologlar alfabetik harfler ile şifreleme yaparlarken, kritoanalistler ise tekrarlanma sıklıkları ile şifreleri çözmeye çalışmaktaydılar. Ayrıca,

185 http://en.wikipedia.org/wiki/Al-Kindi
186 Singh, S. (2002). The Code Book: How to make it, break it, hack it, crack it. New York: Delacore Press

uluslar bu yöntemin çözülme kolaylığının ve yaratacağı tehlikelerin farkına kısa sürede vararak daha farklı şifreleme yöntemleri arayışına girmişler, boşluk, sembol ve harflerde oluşan yöntemler de geliştirmişlerdir. Örneğin; A = Kame, Ω = Internette, 30 = Gizlilik ve Güvenlik ise A Ω 30 = Kame Internette Gizlilik ve Güvenlik olmaktadır.

Son olarak, yukarıda yazanlar doğrultusunda gizli yazının bilimsel olarak dallarını inceleyecek olursak:

,_ Kelime

,_ Steganografi /

/ ,_ Yerine koyma

Gizli Yazı / \,_ Harf

\,_ Kriptografi

\,_ Yerini değiştirme

Her farklı kod, algoritma anlamına gelen bir şifreleme yöntemi olarak düşünülür ve her anahtar belirli bir şifrelemenin tam detayını belirler. Bu bağlamda, algoritma alfabedeki harflerin kod bloğundaki harflerle yerinin değiştirilmesi ve kod bloğu ile yeri değiştirilen harflerin tersi işlemle şifresinin çözülmesi ile gerçekleştirilir. Bir mesajın şifrelenmesi mesajı gönderinin sahip olduğu anahtar ve algoritma ile şifreleyerek, tersi işlemi gerçekleştirecek anahtara ve algoritmaya sahip olan alıcının şifreli mesajın şifresini çözmesi olarak da kısaca özetlenebilir. İletişimin arasına giren saldırgan anahtar ve

algoritmaya sahip değilse mesajı ele geçirse bile şifresini çözeyemecektir. Buna günümüzden bir örnek istenirse gizli ve açık anahtar ile GnuPG'yi[187] gösterebiliriz.

187 https://network23.org/kame/2013/08/28/pgp-kullanin/

23. Amerika'nın Günümüz Kriptografi Standartları Üzerindeki Etkisi

Kriptografi’ye girişin ikinci bölümünde Amerika’nın günümüzde sık kullanılan kriptografi standartları üzerinde nasıl bir etkisi var bunu inceleyeceğiz.

NSA skandallarından sonra kriptografinin ne kadar önemli olduğu, bir insan hakkı olan gizliliği yıllarca ne kadar küçümsediğimiz ve tüm bu gözetim ve izlemelere ne kadar hazırlıksız olduğumuz ortaya çıktı. Bununla birlikte, mesaj içeriğinin şifrelenerek araya girmeler olsa dahi iletişimin sadece gönderen ve alıcı arasında anlaşılır olmasını sağlamak için yıllardır algoritmalar oluşturulmaktadır. Ayrıca, kriptografide sık kullanılan algoritmalar kimler tarafından oluşturuldu, bunların bir standartı var mıdır ve algoritmalar üzerinde kimlerin etkisi vardır görmek iletişimin gizliliği açısından son derece önemlidir. Bu yüzden ilk olarak belli başlı bazı terimlerin neler olduğunu inceleyeceğiz.

NIST

Açılımı; National Institute of Standards and Technology. Adından da anlaşıldığı gibi bir standart kurumudur. Türkiye’de benzer (*ne kadar benzer iş yapıyorlar, tartışılır*) olarak TSE[188] gösterilebilir. Bununla birlikte, 1901 yılında kurulmuş, Amerika’nın en eski fizik laboratuvarlarından da biridir. Genel olarak endüstriyel rekabetçiliğin olumsuzluğunu gidermek için ölçüm standartlarıyla ilgilenmektedirler. Nano düzeyde araçlardan insan yapımı olan en büyük ve karmaşık

188 http://www.tse.org.tr/ana-sayfa

araçlara kadar ölçüm standartlarını desteklemektedirler.

FIPS (Federal Information Processing Standard)

FIPS[189]; Türkçesi Federal Bilgi İşleme Standart'ı olan Amerika Birleşik Devletleri tarafından askeri olmayan devlet kurumları ve devletle iş yapan diğer kurumlar tarafından bilgisayar sistemlerinde kullanılması için geliştirilmiş bir standartlar bütünüdür. FIPS'in amacı tüm federal hükûmetler ve kurumların güvenlik ve iletişimde kullanacakları ortak bir standartın sağlanmasıdır.

Açık-Anahtar Algoritması (Public-key Algorithm)

Açık-anahtar algoritması daha çok asimetrik kriptografi olarak bilinen ve iki farklı anahtar olan açık ve gizli anahtarlardan oluştan bir algoritmadır. Anahtarlar farklı olmalarına rağmen matematiksel olarak birbirleriyle bağlantılıdırlar. Açık anahtar bir mesajın içeriğini şifrelemede veya dijital imzaları doğrulamada kullanılırken gizli anahtar ise şifreli mesajı açar veya dijital anahtarlar oluşturur. Günümüzde sık rastladığımız TSL[190], GPG[191], Diffie-Hellman, RSA ve PGP[192] açık-anahtar algoritmasına örnek olarak gösterilebilirler.

Bu terimleri kavradıktan sonra ikinci olarak sık kullanılan algoritmaların neler olduğu, bunların kimler tarafından ne zaman oluşturuldukları ve üzerinde kimlerin veya hangi kurumların etkilerinin olduğuna bakalım.

---

189 http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard
190 https://en.wikipedia.org/wiki/Transport_Layer_Security
191 https://en.wikipedia.org/wiki/GNU_Privacy_Guard
192 https://en.wikipedia.org/wiki/Pretty_Good_Privacy

AES – The Advanced Encryption Standart

Bilindiği üzere AES[193] (*Rijndael*[194]), simetrik şifre bloğu olup Joan Daemen[195] ve Vincent Rijmen[196] tarafından tasarlanmıştır. DES[197] (*Data Encryption Standart*)'in 56 bitlik küçük bir şifre bloğu olması ve giderek brute force[198] saldırılarına karşı savunmasız kalması yeni bir standartın gerekli olduğunu gösteriyordu. AES ilk 1998 yılında duyrulup yayımlanmış, ardından 2001 yılıda (*Rijndael*) NIST tarafından Advanced Encryption Standart olarak seçilmiştir. Bu seçim süreci birçok farklı tasarımın elenmesinin ardından gerçekleşmiştir. NSA yarışmaya katılan tasarımların hepsini detaylı bir şekilde inceleyip NIST'e son seçimin en güvenli tasarım olması konusunda teknik destek verse de NIST NSA'den bağımsız olarak kendi kararını vermiş ve seçimini de AES'ten yana yapmıştır. Bu yüzden NSA'in AES'e ne bir katkısı ne de üzerinde bir etkisi mevcuttur denilebilir.

RSA – The Rivest, Shamil, Adleman Public Key Algorithm

RSA[199] algoritması 1977 yılında MIT'de[200] kriptografi hocaları olan Ron Rivest[201], Adi Shamir[202] ve Leonard Adleman[203] tarafından tasarlanmıştır. Açık ve gizli anahtar şeklinde ikiye ayrılmatadır. Daha önceside, 1973 yılında bir matematikçi ve İngiliz istihbarat servisi

193 https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process
194 https://en.wikipedia.org/wiki/Rijndael
195 https://en.wikipedia.org/wiki/Joan_Daemen
196 https://en.wikipedia.org/wiki/Vincent_Rijmen
197 https://en.wikipedia.org/wiki/Data_Encryption_Standard
198 https://en.wikipedia.org/wiki/Brute_force_attack
199 https://en.wikipedia.org/wiki/RSA_(cryptosystem)
200 https://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology
201 https://en.wikipedia.org/wiki/Ron_Rivest
202 https://en.wikipedia.org/wiki/Adi_Shamir
203 https://en.wikipedia.org/wiki/Leonard_Adleman

GCHQ[204] çalışanı olan Clifford Cocks[205], benzer bir algoritma tasarlamış ve belgelerinin yüksek derecede gizlilikleri yüzünden 1998 yılında keşfedilmiştir. Clifford Cocks uygulanması için dönemin pahalı bilgisayarlarına ihtiyacın olduğu, çoğunluk meraktan tasarladığı ve uygulanmadığını belirtmiştir. RSA hem akademik çevreler hem de NSA tarafından detaylı bir şekilde analiz edilmiştir. Bununla birlikte, NSA'in RSA'nın tasarlanmasında veya geliştirilmesinde herhangi bir katkısı yoktur.

Diffie/Hellman/Elliptic-Curve Diffie-Hellman/The Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman[206] algoritması 1976 yılında Stanford Üniversitesi'nde kriptografi hocaları olan Withfield Diffie ve Martin Hellman tarafından tasarlanmıştır. GCHQ çalışanları olan Malcolm Williamson[207], Clifford Cocks ve James Ellis[208] tarafından birkaç yıl önce bulunmuş fakat yayımlanmamıştır. Diffie-Hellman'ın eliptik eğri sürümü ise bağımsız olarak 1985 yılında Amerikalı kriptologlar Victor Miller[209] ve Neal Koblitz[210] tarafından bulunmuştur. 2002 yılında Hellman, açık-anahtar kriptografisinin bulunmasında büyük katkısı olan Ralph Merkle'nin[211] de tanınması için algoritma adını Diffie-Hellman-Merkle olarak değiştirmiştir. NSA, potansiyel olarak zayıf olan eliptik eğri parametrelerinin NIST standartları içerisinde yer almamasını sağlamıştır.

---

204 https://en.wikipedia.org/wiki/Government_Communications_Headquarters
205 https://en.wikipedia.org/wiki/Clifford_Cocks
206 https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
207 https://en.wikipedia.org/wiki/Malcolm_J._Williamson
208 https://en.wikipedia.org/wiki/James_H._Ellis
209 https://en.wikipedia.org/wiki/Victor_S._Miller
210 https://en.wikipedia.org/wiki/Neal_Koblitz
211 https://en.wikipedia.org/wiki/Ralph_Merkle

DSA/ECDSA – The Digital Signature Algorithm/Elliptic Curve DSA

DSA[212] algoritması dijital imzalar için bir FIPS standartıdır. 1991 yılında NIST tarafından dijital imza standarlarında (*DSS*) kullanılması için teklifte bulunulmuş ve 1993 yılında kullanılmaya başlanmıştır. Bununla birlikte, DSA 1991 yılında eski bir NSA çalışanı olan David Kravitz tarafından tasarlanmıştır. Ayrıca NSA, Eliptik Eğri DSA ya da ECDSA olarak bilinen diğer bir sürümünü de tasarlamıştır. DSA, akademik çevreler tarafından analiz edilmiştir.

SHA-1/The Secure Hash Algorithm 1

Ron Rivest tarafından tasarlanan MD5[213] algoritmasının uzun bir benzeri ve SHA-0 algoritmasının düzeltilmiş hali olan SHA-1[214], NSA tarafından tasarlanmıştır. SHA-0 ise 1993 yılında bir standart haline gelen NSA tasarımıdır. Fakat, 1994 yılında NSA kriptologları SHA-o tasarımında güvenliği azaltan bir sorunla karşılaştıklarında, bu açığı hızlıca kapatmak için bir NIST standartı olan SHA-1′le yer değiştirmişlerdir. Ayrıca, SHA-1 akademik çevreler tarafından analiz edilmiştir. Öte yandan, uzun yıllardır hem NIST hem de NSA SHA-2′nin kullanılmasını tavsiye etmektedir.

SHA-2/The Secure Hash Algorithm 2

NSA, dört farklı uzunluktan oluşan (*224, 256, 384 ve 512 bit*) hash algoritmarları içeren SHA-2‘yi[215] tasarlamış ve NIST tarafından yayımlanmıştır. SHA-2 daha uzun hashlere sahip olduğu için SHA-1′e göre daha iyi bir güvenlik sağlamaktadır. Ayrıca, SHA-1′in tasarımdan

212 http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
213 http://en.wikipedia.org/wiki/Md5
214 http://en.wikipedia.org/wiki/Sha-1
215 http://en.wikipedia.org/wiki/Sha-2

kaynaklanan bazı algoritma açıklarına karşı daha iyi bir savunma oluşturur. Bu algoritmanın bir FIPS standart olması ise 2002 yılında gerçekleşmiştir. SHA-2 de akademik çevreler tarafından analiz edilmiştir.

Görüldüğü üzere, bizlerin kriptografide kullandığı bazı algoritmalar tasarlandıktan sonra yayımlanmış ve bilim adamları, matematikçiler, mühendisler vd. tarafından analiz edilmiştir. Ayrıca, bu algoritmalar için belirli standartlar oluşturulmuş ve güvenilirliği için onay verilmiştir. Öte yandan, günümüzde sık kullanılan bu algoritmalar üzerinde NSA ve GCHQ gibi istihbarat kurumlarının etkisi net olarak görülmekte, bu algoritmalara benzer algoritmalar oluşturdukları ve yayımlamadıkları da bilinmektedir. Bilim etiği, planlı ve sistemli olarak toplanan verilerin analiz edilmesi, yorumlanması, değerlendirilmesi ve başkalarının da geliştirmesini içerse de gizliliğin istihbarat kurumlarının tekeline bırakılmaması gerektiğinin önemi bir kez daha gözler önüne sermektedir. Çünkü, iletişimin gizliliğini sağlamak amacıyla kullanılan birçok kriptografi algoritmasında istihbarat kurumlarının etkisi veya katkısından ziyade bireylerin daha açık ve daha özgür olarak tasarlanmış, analiz edilmiş ve geliştirilmiş algoritmalara ihtiyacı vardır. Bu, hem iletişimin gizliliğine olan güveni artıracak hem de asıl amacı gizliliği ortadan kaldırmak olan NSA ve GCHQ gibi kurumların küresel gözetim ve izlemesinden daha iyi bir şekilde korunmayı sağlayacaktır.

24. Twister

> Twitter sık sık erişeme engelleniyor mu? Twitter hesapları takip mi ediliyor? Twitter'a erişemezsek ne mi olacak? Bu soruların cevaplarını Twister'da bulabiliriz.

Twister[216]; Miguel Freitas tarafından yazılmış ve merkezsizleştirilmiş özgür yazılım olan bir P2P mikroblog platformudur. Platform bağımsızdır. GNU/Linux, Windows, Android ve Mac OS için kurup kullanabilirsiniz. Bittorrent ve Bitcoin benzeri bir yapıda çalışmaktadır. Merkezsizleştirilmiş olması kimsenin erişime engelleyemeyeceği, sansürleyemeyeceği ve ifade özgürlüğünü elinizden alamayacağı anlamına gelmektedir. Bununla birlikte, noktadan noktaya şifreleme kullandığı için iletişim (*tüm iletişim değil, özel mesaj*) gizlice izlenemez. IP kaydınız tutulmaz. Ayrıca, açık kaynak ve ücretsizdir.

Nasıl Çalışıyor?

Twister; 3 katmandan oluşan bir ağ yapısına sahiptir. Birinci katmanda kullanıcı hesaplarının oluşturulması ve doğrulanması için Bitcoin protokolü kullanılır. Aslında bu tamamen Bitcoin protokolünün kullanılmasından ziyade blok zincirini ifade eder. Bu da şu demektir; blok zincirleri noter görevi görürler ve oluşturulan kullanıcı adının kime ait olduğu ve hangi anahtar çiftine sahip olduğunu onaylarlar. Twister'da doğrulama ve şifrelemeyi oluşturan nokta burasıdır. İkinci katmanda DHT protokolü bulunmaktadır. DHT, üçüncü katman için istemcilerde kullanıcı kaynakları olarak anahtar/değer ve tracker konumlarını barındırır. Son katmanda ise birbirlerini takip eden

216 http://twister.net.co/

kullanıcılar için Bittorrent yapısına dayanan bir bildirim (*girdiler, uyarılar, cevaplar vs gibi*) sistemi vardır. Daha detaylı bilgiye Miguel Freitas yazdığı makaleden[217] ulaşabilirsiniz.

Kurulum

Kurulum GNU/Linux içindir ve oldukça basittir. Diğer sistemler için lütfen buraya[218] bakın. İlk olarak terminali açalım ve derleme için gerekli paketleri kuralım:

kame ~ $ sudo apt-get (*pacman -S, emerge -av vs*) openssl db boost miniupnpc

Daha sonra Twister çekirdeğini kuralım:

kame ~ $ git clone https://github.com/miguelfreitas/twister-core

kame ~ $ cd twister-core

kame ~ $ ./bootstrap.sh

kame ~ $ ./configure --enable-logging --enable-debug

kame ~ $ make

kame ~ $ sudo make install

Son olarak Twister için HTML kullanıcı arayüzünü kuralım:

kame ~ $ mkdir .twister

kame ~ $ cd .twister

217 http://arxiv.org/abs/1312.7152
218 http://twister.net.co/?page_id=23

kame ~ $ git clone https://github.com/miguelfreitas/twister-html.git html/

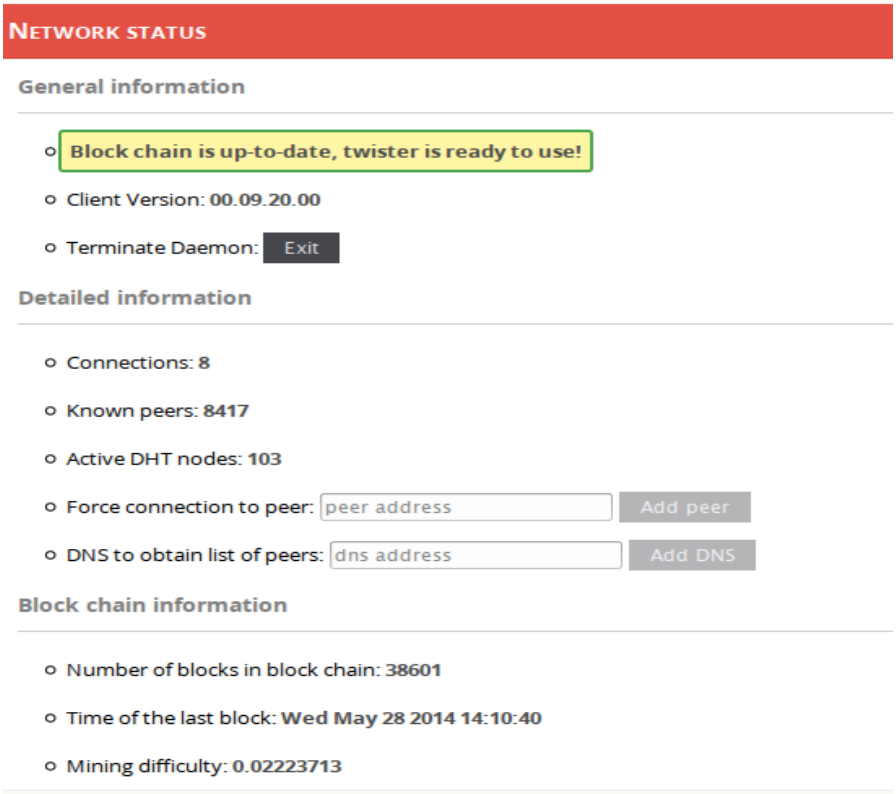
Çalıştırma

Kurulum sorunsuz bir şekilde tamamlandıysa aşağıdaki komut satırını herhangi bir değişiklik yapmadan çalıştırıyoruz:

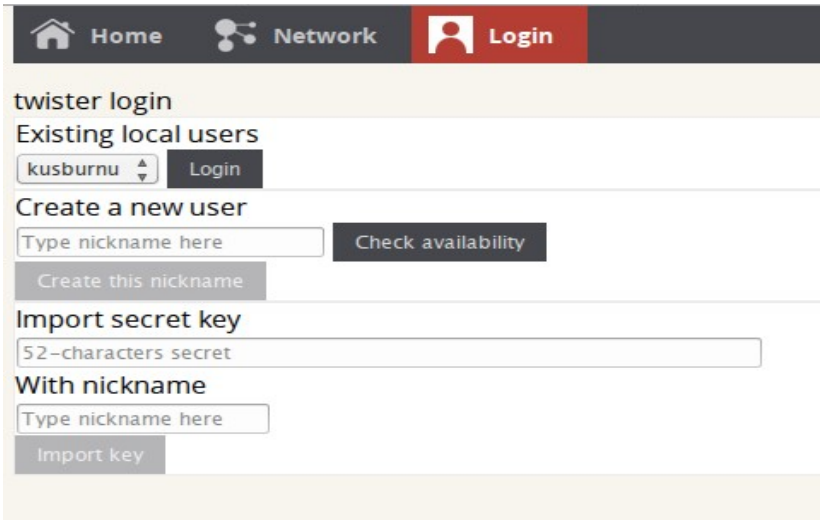
kame ~ $ ./twisterd -daemon -rpcuser=user -rpcpassword=pwd -rpcallowip=127.0.0.1

Adres: http://127.0.0.1:28332/home.html

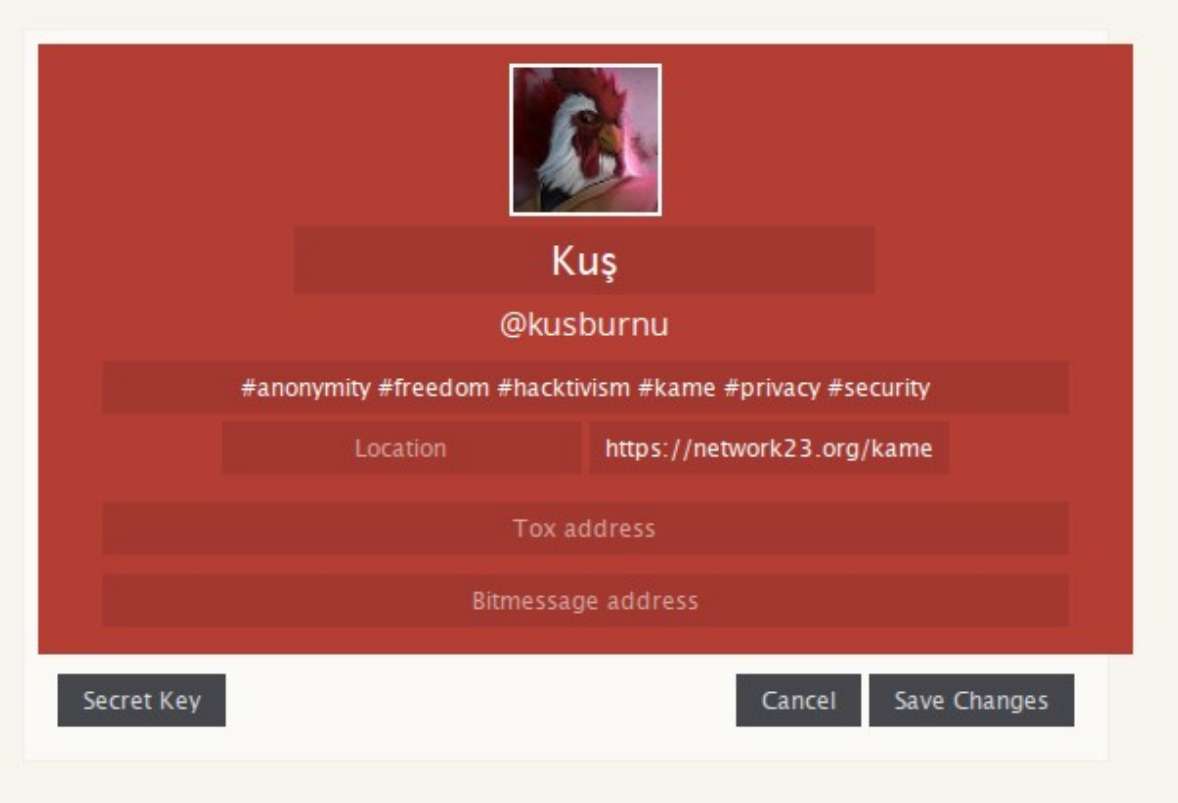
Blok zincirleri eski olduğu için bir süreliğine güncelleştirme yapacaktır. Ağ durumuna Network sayfasından bakabilirsiniz.



Görüldüğü üzere blok zinciri güncel ve Twister kullanılmaya hazır. Bu sayfanın alt kısmında tıpkı Bitcoin'de olduğu gibi madencilik yapabilirsiniz. Madenciliğin ne gibi bir katkısı var? Blok zincirlerinin zorluk derecesi arttıkça daha yüksek bir güvenlik sağlanıyor ve ne kadar çok kişi madencilik yaparsa o kadar çok yeni zincir oluşturularak kullanıcıların zincirlere kayıt süresi azalıyor. Güncelleştirme tamamlandıktan sonra Login sayfasından yeni bir kullanıcı oluşturabilirsiniz.



Kullanıcı oluşturduğunuzda kullanıcı adınıza ait ve saklamanız gereken bir adet anahtar da oluşturulacaktır. Böylece farklı sistemlerde veya cihazlarda Twister kullandığınızda kendi hesabınızı bu anahtar ile aktarabileceksiniz. Profil sayfasında profil fotoğrafı, mekan, website adresi gibi profilinize ait bilgileri girip kaydedeceksiniz. Burada dikkat etmeniz gereken kayıt bağlantısının belirli bir süre aktif olmamasıdır. Çünkü, blok zincirine kayıt olunması biraz zaman alıyor. Kullanıcı adınızı oluşturduktan sonra belirli bir süre bekleyin.



Kullanıcı kaydı da gerçekleştirildikten sonra artık siz de mikrobloglama başlayabilirsiniz. Twister'la ilgili bilemeniz gereken bir kaç nokta var. Bunları sıralayacak olursak:

- Twister'ın yapısı gereği sizleri takip eden kullanıcıları göremiyorsunuz. Ama takip ettiğiniz kullanıcılar görülmektedir.
- Kullanıcı adınız için oluşturulan anahtarı kaybederseniz kullanıcı adınızı geri alma şansınız kalmaz.
- Unutulmaması gereken nokta da Internet trafiğiniz gözetim altında ise Twister sizlere gizlilik sağlayamaz.
- Twister, secp256k1 adında Bitcoin ile aynı eliptik eğri parametresini kullanmaktadır. NSA'in sec256r1 parametresini

kırdığı biliniyor. Fakat, aynı durum Bitcoin ve Twister'da kullanılan parametre için -şimdilik- geçerli değildir.

Son olarak, Twister Türkçe dile de sahiptir. Daha çok ilgi görmeyi hakediyor ve özellikle engellemeler yüzünden gittikçe yalama olan Twitter gibi platformlar yerine tercih edilebilir. Bir diğer durum da Twitter kullanıcılarının ifade özgürlüğü haklarını mahkemelerde savunsa da, NSA ve PRISM ile işbirliği yapmasa da ifade özgürlüğünü bir şirketin eline bırakmak yanlış olacaktır. Bu yüzden bireylerin Twistter gibi uygulamalara önem vermeleri ve desteklemeleri gerekmektedir.

25. Netclean ve URL Tabanlı Engelleme

> 5 saniye içinde içeriği silmek mi? Bir dakika, ben mi her şeyi yanlış anladım?

İlk olarak Wikileaks'in bugün paylaşmış olduğu tweetlere bakalım:

1. #Sweden to sell #Turkey $40m internet censorship system 'netclean' http://www.hurriyetdailynews.com/turkeys-top-soldier-warns-against-social-media-as-govt-to-purchase-software-against-illegal-shares.aspx?pageID=238&nid=67178&NewsCatID=341 #svpol[219]
2. Context: Censored paper covering #Sweden's "Netclean" internet censorship system https://wikileaks.org/wiki/Removed_paper_on_Internet_censorship_trails_in_Australia,_NZ,_UK_with_NetClean_Whitebox,_2009 more: https://twitter.com/wikileaks/status/475564846524940288[220]

Netclean kendi yaptığı tanıma[221] göre; daha güvenli toplumlar için dijital ortamları tarayan, analiz eden ve içerikleri engelleyen yazılımlar sunan bir firmadır. Bununla birlikte, temel amacı çocuk pornosuna karşı mücadele etmektir. Ayrıca, yazılımları dünya çapında devletler, çok uluslu şirketler, İSS'ler ve kanun uygulayıcılar tarafından tercih edilmekte ve kullanılmaktadır. Çok yakın bir tarihte (30 Mayıs 2014) Türkiye'nin İsveç'ten Netclean firmasına ait WhiteBox ürününü 40

219 https://twitter.com/wikileaks/statuses/475564846524940288
220 https://twitter.com/wikileaks/statuses/475573626507640832
221 https://www.netclean.com/en/about-us/

milyon Euro vererek alacağına dair haberler paylaşıldı. Bununla ilgili olarak Sabah gazetesinden bir kısa alıntı yapalım[222]:

Özel hayatın gizliliğini koruyarak kişisel hakların ihlal edilmemesini isteyen hükümet, Twitter üzerinden yapılan yasa dışı paylaşımlara çözüm bulmak için kolları sıvadı. Twitter üzerinden paylaşılan yasadışı fotoğraf, görüntü ve bilgileri hemen silmek için Türkiye yazılım alıyor.

17 Aralık 2013 yolsuzluk operasyonu ile hükûmetin yaşadığı şok ve istihbaratın yetersizliği, Internet'in paylaşım ve insanlara ulaşım konusundaki büyük esnekliği ve bunu engelleyebilmek için de yetersiz bir altyapı Türkiye'yi yeni yazılımlar arayışına itmiş gözükmektedir. Bunun arkasında ise her zamanki gibi özel hayatın gizliliği ve kişisel hakların ihlal edilmemesi gereği yatmaktadır. Diğer taraftan, gizlilik hakkına bu kadar duyarlı olan hükûmetin 5651 sayılı kanunu hangi amaçla uygulamaya koyduğu ise çelişkinin bir boyutudur.

Yapılan araştırmalar sonunda Twitter'daki istenmeyen ve hakkında mahkeme kararı bulunan içerikleri engellemenin yolunun bulunduğu savunuluyor.

İstenmeyen içerikler ve hakkında mahkeme kararı bulunan içerikler diyerek ikiye ayırmak bir art niyet olarak görülmemelidir. Hükûmet, istemediği içeriği kaldırabilmek için 5651 ile altyapı hazırlamış fakat, kontrol edemediği alanlardaki istenmeyen içeriği de URL tabanlı engelleme ile baş etmek istiyordu. Erişim Sağlayıcıları

222 http://www.sabah.com.tr/Ekonomi/2014/05/30/twitterda-net-temizlik-basliyor

Birliği ile bir çatı altında toplanacak olan İSS'ler, URL tabanlı engelleme için kurmaları gereken altyapıların yüksek maliyetli olması ve son yaşanan Netclean gelişmesi ile tek bir noktadan URL tabanlı engelleme gerçekleştirileceğine işaret etmektedir. Bu da daha önce de bahsettiğim üzere trafiğin tek bir noktada (Erişim Sağlayıcıları Birliği) toplanıp aynı noktada engellerin yapılacağı anlamına gelmektedir. Haberin son kısmında ise:

40 milyon euroluk yazılım sayesinde Twitter'da paylaşılan çocuk pornosu gibi illegal linkler anında temizleniyor. Temizleme işlemi ise yazılıma girilen anahtar kelimelerle gerçekleşiyor. Yazılımın birçok kişinin mağduriyetini gidermesi bekleniyor.

Dünya çapında izleme ve gözetimin 5 gözü olduğu söylenmektedir. Bunlar; Amerika, İngiltere, Avusturalya, Kanada ve Yeni Zelanda'dır. Bununla birlikte, Yeni Zelanda merkezli ve Avusturalya, İngiltere ve Yeni Zelanda'daki sansür sistemin arkasında bulunan firma olan Watchdog International'in Whitebox ile ilgili yayınlamış olduğu belgeye kısaca bir göz atalım:

- Whitebox, bir liste mantığı ile filtreleme gerçekleştiren URL tabanlı engelleme ve filtreleme yazılımıdır.
- Engellenmesi istenen URL'ler bu listelere girilerek gerçekleştirilir.
- DNS zehirleme filtreleri ile kullanılabilmekte fakat, tavsiye edilmemektedir.
- Bir proxy sunucusu ile çalışabilir fakat, tavsiye edilmemektedir.
- Çocuk pornosu gibi küresel konularda URL listeleri diğer

ülkelerle paylaşılmalı ve erişime açık olmalıdır. Böylece daha etkili bir engel sistemi ve güncel URL listesi oluşturulabilir.

Öncelikle Whitebox, bir URL temizleme ve içeriği silme aracı değildir. Haberde bahsedilen temizlik işlemi URL'lere ait içeriğin silinmesine işaret ederken Whitebox'ın gerçekte yaptığı URL listesi ile URL tabanlı engelleme gerçekleştirmektir. Bir filtreleme yapmaktadır, yüksek trafiğe sahip websitelerde (*örneğin, Youtube*) kullanılması tavsiye edilmemekte, DNS zehirleme filtreleri ile kullanılabilmekte, bir proxy sunucusu ile filtreleme yaparak hedef URL'ye erişim sağlayabilmektedir. Hürriyet Daily News'in konuyla ilgili haberine[223] gelecek olursak:

"Different threats have occurred in the new world order. Countries are being subjected to colorful changes and seasonal revolutions formed by information technology and social media, Özel said.

Necdet Özel, yeni dünya düzeninde farklı tehditlerin ortaya çıktığını ve bilişim teknolojileri ve sosyal medyanın ülkelerde yaşanan dönemsel ayaklanmalarda etkili olduğunu belirtmiş. Bunun için de hükûmeti sosyal medyadaki yasalara aykırı paylaşımları engellemek amacıyla bir yazılım alması konusunda da uyarmış. Haberin devamında, İçişleri Bakanı Efkan Ala'ya yazılımla ilgili sunum gerçekleştirildikten sonra İçişleri Bakanlığı tarafından alıncağını belirtilmiştir.

223 http://www.hurriyetdailynews.com/turkeys-top-soldier-warns-against-social-media-as-govt-to-purchase-software-against-illegal-shares.aspx?pageID=238&nid=67178&NewsCatID=341

Son günlerde yaşanan Internet'teki yavaşlığı da dikkate alırsak yeni bir URL tabanlı engelleme sistemimiz hayırlı olsun diyebiliriz. 40 milyon Euro gizlenmeye çalışılan[224] çocuk felci salgınına harcanabilir miydi? Ama devletin bir süprizle karşı karşıya kalmaması için hükûmet nelerden ödün verebilir? Bir de orası var.

224 http://www.sendika.org/2014/06/cocuk-felci-salginiyla-kacak-mucadele/

İletişim

Twitter: https://twitter.com/songuncelleme

E-posta: kusburnu@riseup.net

Blog: https://network23.org/kame

Bağış: 17qsapk4FzU9hpQP65GKmDe7WZrAv6J3vZ (*BTC*)