CITIZENLAB Derin Paket Analizi Aldatmacası

Yazıma başlarken biraz kendimden bahsetmek istiyorum. 2005 yılında bilgisayar mühendisliği alanında lisans eğitimini tamamladıktan sonra Gazi Üniversitesi'nde araştırma görevlisi olarak akademik hayata atıldım. Bu serüvenin 2014 yılında doktorayı bitirinceye kadar devam etmesi gerekirken doktoradan sonra 4 yıl daha araştırma görevlisi olarak çalışmak zorunda kaldım. Bu süreçte ABD'de veri madenciliği alanında doktora sonrası araştırmalarda bulundum, yurda döndükten sonra kadro başvurularında bulunurken daha 2 ay önce yardımcı doçent unvanını almıştım ki bir de baktım doktor öğretim üyesi olmuşum. Akademik hayatın zor ve kolay taraflarında bir denge tutturmuşken önümde zor bir doçentlik sürecinin beni beklediğini biliyorum. Bu süreçte sadece yayın yapmak değil aynı zaman da kaliteli yayın çıkartmak hedeflerim arasında.

İşte bunun gibi bir konu arayışım esnasında çalışma alanım olan siber güvenlik konusu karşıma şakayla karışık bir site çıkarttı. Bende ilk bu konudan başlayarak insanlığa daha faydalı olmak için bir blog oluşturmaya karar verdim. Akademik yayınlar sadece üniversite camiasına ulaşırken internet erişimi olan herkese ulaşma fikri daha cazip geldi.

Bu ilk blog yazımda alanımla ilgili bilimsel araştırma yaparken karşılaştığım Citizen Lab (https://citizenlab.ca) isimli oluşumdan bahsedeceğim zira adı her ne kadar Avrupa'da insan hayatının kalitesini arttırmaya yönelik bir proje başlığı gibi görünse de anlam veremediğim bir şekilde Türkiye ile alakalı ciddi iftiraların olduğu Kanada merkezli bir araştırma laboratuvarına ait bir oluşum. Yalnız iddiaları o kadar abartılmış durumdaki Türkiye'yi topun ağzına koymak için teknolojinin ve internetin kendi iç dinamiklerini gerçekte olmayan kurallarla dahi süslemiş bir site ve sözde teknik olarak elde ettikleri çıktılardan oluşturulmuş safsata bir raporu var.

İsterseniz öncelikli olarak arkadaşları tanıyalım. Araştırmaya önderlik eden kişi Ronald J. Deibert maalesef bir bilgisayar bilimcisi değil, iddia ettikleri üzere ülkelerin ağ trafiğinin dinlenmesi ve izlenmesi işini yapan üstelik Twitter'da 40 bine yakında takipçisi olan bir araştırma grubunun başında olan kişi ister inanın ister inanmayın bir siyaset bilimcisi profesörü (Professor of Political Science). İnternet, siber uzay, anahtarlama ve yönlendirme cihazları, OSI katmanları, SSL ile kriptolu TCP paketlerinin incelenmesi işlerini yapan Türkiye hakkında akla hayale sığmayacak

iddialarda bulunan ve Toronto Üniversitesi'nin resmi araştırma grubu olduklarını özellikle beyan eden bir laboratuvarın başında sayısal dendiğinde 4 işlem hesap makinesini açmanın ötesine bilimsel olarak geçemeyecek bir kişinin bulunması bile iddiaların ne kadar siyaset dolu olduğunu, tam bir karalama kampanyası olduğunu gösteriyor.

İddialar her ne kadar bilgisayar bilimcisi olmayan kişilerce ortaya atılmış olsa da bu blogun amacı kimseyi yalanlamak değil aksine doğru olduğu iddia edilen yanlışlara farklı bir bakış açısı katmak. Genel de akademik yayınlarda körü körüne iddialar verilmez aksine tartışılır direkt sonuç yazılmaz çalışmanın zayıf kaldığı yönlerde verilir. Bu raporda ise bu tip bir bakış açısından imtina edilmiş ve sanki raporu başkası yazmış ama altına başkaları imza atmış gibi duruyor. Neden bu fikre kapıldığım sorusuna gelecek olursak. Araştırma grubunun başındaki Ronald J. Deibert haricinde Staff ve Research Fellows başlıkları altında birçok kişinin adı yer alıyor. Türkçe'de Staff her ne kadar idari personel anlamına gelse de o bölümde Kıdemli Araştırmacılar da yazılmış. Özellikle @utoronto.ca e-posta adresi olan Jakub Dalek, Ivy Lo, Sarah McKune, Irene Poetranto ve Adam Senft, Staff bölümü altında bulunuyor. Bu kişilerin görev dağılımlarına baktığınız zaman Jakub Dalek için Senior Researcher yani kıdemli araştırmacı denmesine rağmen internet aramalarında kendine Toronto Üniversite üzerinden ulaşmak mümkün olmuyor, Ivy Lo için Business Officer yani idari bir pozisyonda olduğu, Sarah McKune için Senior Researcher yani kıdemli araştırmacı denmesine rağmen internet aramalarında ekoloji doktorasının olduğu, Adam Senft için ise Operations Manager yani yine bir idari kadroda bulunduğu anlaşılıyor. Asıl teknik araştırmayı yaptırması gereken Faculty pozisyonu altında Ronald J. Deibert'den başkası bulunmuyor. Faculty altında bulunması gereken hocaların araştırma yaptıracakları kişiler ise Research Fellows (2017-2018) başlığı altında verilmesine rağmen bu bölümde yer alan 20 araştırmacıdan hiç kimsenin Toronto Üniversitesi ile bağlantısı bulunmuyor. Araştırma pozisyonunda yer alan kişilerden de sadece 3 kişinin kişisel e-posta adreslerinin verildiği görülüyor. Buradaki ironiyi anladığınızı düşünüyorum; Toronto Üniversitesi'nin Türkiye'ye sayısız iftira ve hakaretlerde bulunan ve sözüm ona Twitter'da 40 bin takipçisi bulunan araştırma laboratuvarında çalışan Toronto Üniversitesi bağlantılı araştırmacı yok, idari ve yönetici pozisyonlarında çalışan kişilerin ise bilgisayarın b'si ile uzaktan yakından alakaları yok.

Belki bu kadar kanıt dahi ülkemiz üzerinde oynanan oyunları ortaya koymak için yeterlidir. Ancak bu blogun amacı daha öncede dediğim gibi bize atılan iftiralara onlar gibi değil teknik ve bilimsel gerçekler ile cevap vermek, bakış açısı katmak ve ışık tutmak olmalıdır.

Türkiye iftiralarının olduğu araştırma raporunun başlığı Kötü Trafik (Bad Traffic). Belki inanmayacaksınız ama yazıyı yazanlar "Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert". Önceki bölümde Jakub Dalek, Sarah McKune ve Adam Senft hakkında konuşmuştuk. Bu Staff yani idari personeller anlaşılan bir gece de akademik bilgisayar bilimleri araştırmacılığına terfi etmişler. Diğer kişilerden sadece Bill Marczak ile ilgili bilgilere ulaşılırken John Scott-Railton ve Ron Deibert için biraz daha derine inmek gerekiyor. Ron Deibert'in bizim siyaset bilimi profesörü olan müdürün kısa adı olduğunu varsayarsak John Scott-Railton'da araştırdığınızda Linkedin sayfasında kamu yönetimi doktoralı bir kişi olduğu anlaşılıyor. Bu kişilerin neden Kanada'da bir araştırma grubu kurdukları net olmamakla birlikte direkt olarak siyasetçi, kamu yönetimcisi vs. akademik alanlarda çalışan kişilerin bilgisayar bilimlerinde teknik raporlar vermeleri anlaşılabilecek alışılagelmiş bir olay değil. Elbette çok disiplinli çalışmalar yapılabilir ama sadece teknik bilginin ve çok net iftira ifadelerinin olduğu bir rapor da 1 bilgisayar bilimcisi ve 5 sosyal kökenli kişi bir araya gelmiş anlamak zor. Bu hiçbir standart altında çok disiplinli kabul edilemez.

Teknik olmayan kişilerce yazılmış teknik rapor, şu cümle ile başlıyor; "iki ülkede kullanılan Sandvine/Procera Networks Derin Veri Analizi (DPI) cihazlarının (bir diğer adıyla MiddleBoxların) muhtemelen devletler ya da internet hizmet sağlayıcılar (ISP) tarafından kötücül ya da şaibeli amaçlar için kullanımını internet taraması yoluyla nasıl ortaya çıkardığımızı anlatmaktadır" deniliyor. Akla gelen ilk soru Kanada'dan Türkiye ağını nasıl dinledikleriyle ilgili çünkü iddiaları şu cümle ile pekişiyor "İnternet taramamız sonucunda Türk Telekom ağı üzerinde derin veri analizi (DPI) kullanan MiddleBoxlar tespit ettik" cümlesinde anlam kazanıyor. Kanada'dan Türk Telekom ağını dinlemişler, belki yazımı okuyanlar teknik konulara hakim olmayabilirler ama hayatımda okuduğum en saçma ve en anlamsız cümlelerden birini okuyorsunuz. İnternet sıradan bir gözle baktığınız zaman A noktasından B noktasına ulaşmanızı sağlayan sanal geçitlerden ve fiziksel kablolu cihazlardan oluşan bir topoloji olabilir. Ancak, bırakın bir ülkenin hattını dinlemeyi eviniz de oluşturduğunuz 3 bilgisayarlı bir ağ da dahi trafik

dinlemesi ve paket analizi yapmanız teknik olarak mümkün değildir. Günümüz de eski tip HUB yapısında anahtarlama cihazları değil son 20 yıldır akıllı anahtarlama dediğimiz Switch cihazları kullanılmaktadır. Dolayısıyla aynı ağa bağlı olduğumuz halde ben nasıl komşunun gelen giden ağ paketlerini inceleyemiyorsam, evimde kullandığım masaüstü bilgisayardan eşimin dizüstünden yaptığı görüşmeleri dinleyemiyorsam, Kanada'da oturan bir siyaset bilimcisi de benim ülkemin ağ paketlerini izleyemez. Dolayısıyla derin veri analizi (DPI) ile paket enjeksiyonu cihazı çok şaşalı bir isim olmaktan öteye gidememektedir. DPI kendi kişisel bilgisayarınız da kullandığını paket inceleme programı olan WireShark yazılımından öteye gidemeyecek bir teknolojidir. Buna dair nedenleri anlamak için biraz internetin nasıl doğduğuna bakmamız gerekmektedir.

İlk internet Darpa tarafından 1983 yılında geliştirilen ARPANET isimli bir ağ ile hayata geçmiştir. Zaman içerisinde güvenlik duvarları(FW), saldırı tespit sistemleri(IDS), saldırı önleme sistemleri(IPS), kablolu/kablosuz/optik akıllı cihazlar, Layer 3 Anahtarlar(Switches), Yönlendiriciler(Routers) gibi sayısız teknolojik harikalar hayatımıza girmiştir. Tüm bu yazılım ve donanım cihazları hayatımızı kolaylaştırdığı kadar internetin daha güvenli ve daha erişilebilir hale gelmesinde önemli roller almıştır. Teknik raporda MiddleBox adında cihazların Türk Telekom içerisinde tespit edildiği ve bunların kötücül yazılımlar(malware) ile zenginleştirilmiş yasal Windows programlarına eklenerek kullanıcıların verilerini çalmak ve izlemek için kullanıldığı gibi akla hayale sığmayacak bir iddia bulunmaktadır. Öncelikle şunu belirtmek gerekir ki MiddleBox genel bir kelimedir. Kullandığımız güvenlik duvarları da büyük kurumlarda örneğin çalıştığım üniversite de kullanılan NAT cihzları da bir MiddleBox cihazıdır. Network Address Translator(NAT) günümüzde IPv4 uzayının yetmediği tüm dünyada sayısız kurum da kullanılan bir teknolojidir. Amacı ise çok basit şekilde; yerel ağ üzerinde bulunan bir cihaz internete çıkmak istediğinde bu bilgisayarın yerel IP adresi ile dış dünyada kullanılacak IP adresini buluşturmaktır. Bu sayede tükenen IPv4 adres uzayından tek bir IP adresi binlerce cihaz tarafından tek bir ağ geçidi üzerinden internete sorunsuz çıkabilmektedir. MiddleBox şaşalı adının altında dünyada her gün binlerce servis sağlayıcı(ISP) ve milyonlarca farklı kullanıcı tarafından kullanılan cihazlar olarak karşımıza çıkmaktadır. Türk Telekom'da, Gazi Üniversitesi'nde veya Toronto Üniversitesi fark etmeksizin zorunluluk nedeniyle kullanılmaktadır. Yazının başında Derin Veri Analizi (DPI) cihazları denmesini anlayabilirim ama bir diğer adıyla MiddleBoxlar denmesini anlamak mümkün değildir. Ben psikolog değilim ama bilmediğim güzel bir ismi ve kısaltması olan cihaz ile ne

olduğunu bildiğim gerçek bir cihaz adı yan yana geldiğinde benliğim ilk cihazında doğru olması gerektiğini söyler. Bu raporu yazan kişilerin akademik yeterliliklerine baktığım zaman insan psikolojisinde üst perdeden iş yaptıklarını görüyorum. Derin Veri Analizi (DPI) cihazları vardır ama engelleme için evet, trafiği uygun içeriğe yönlendirmek için evet ama paketin içine enjeksiyon yaparak casus yazılım yerleştirmek için hayır, bu son derece saçma ve hiçbir bilimsel/teknik tarafı olmayan bir iddiadır.

Yine de bir an olsun olaya kuşkucu yaklaşarak Türk Telekom'da MiddleBox adında Derin Veri Analizi (DPI) ile Kanada'dan buraya kadar anlaşılabilecek cihazlar olduğunu hayal edelim. Çünkü iddia daha doğrusu iftira bu cihazların Türkiye, Mısır ve Suriye üçgeninde Türk Hükümetinin Casus Program Kullanmasını sağladığı yönündedir. İddia olduğu üzere ben bilgisayarıma resmi sitesinden Avast Antivirus, CCleaner, Opera, ve 7-Zip gibi ücretsiz yazılımlar indirmek istediğimde indirilmek istenen dosya sanki üreticinin sitesinden değil Türk hükümeti tarafından kötücül/casus yazılım eklenen kurulum dosyalarına yönlendirildiği, söylenmektedir.
Bu iddia da ilk aklıma gelen 4 problem göze çarpmaktadır. İlk problem hiç kimse 7-Zip sitesine adresini bilerek girmemektedir. Herkes bu ve benzeri siteleri en bilinen Google arama motoruyla aratarak yükleme dosyalarına ulaşmaktadır. Google HTTP ile değil HTTPS ile çalışmaktadır. Bir diğer ifade ile aratılan tüm kelimeler kriptolu/şifreli olarak internet üzerinden geçmektedir. Kullanılan şifreleme tekniği ECDSA P256 modelidir. Kaba Kuvvet(Brute Force) gibi internet hızında çalışmayacak algoritmalar kullanılsa bile Google üzerinde akan trafiği analiz edebilmek için Türk Hükümetinin RSA şifrelemeyi çözen tekniği bulmuş olması gerekir. Dolayısıyla RSA ile korunan bilgilere erişmek günümüz de teknik olarak mümkün değildir. Bu işlem 1 kişinin veri paketleri için dahi kaba kuvvet saldırısıyla aylar/yıllar sürebilecekken aynı anda milyonlarca kişinin ağ trafik paketini analiz etmek sonsuzluğa yakın bir zaman ve Google yada Microsoft'un dahi elinde olmayan bir işlem gücü gerektirecektir.

İkinci problem ise üreticiler yazılımlara ait hash(özet) değerlerini bu ve benzeri ataklara karşı yayınlamaktadır. Özet fonksiyonları bilgisayar bilimlerinde kullandığımız hiçlik yani null değerinden terrabaytlar mertebesinde dosyalara kadar sabit uzunlukta matematiksel çıktılar üreten hem doğrulama hem de şifreleme teknikleri içinde kullanılan algoritmalardır. Kullanım amacına yönelik en bilinen özelliği bir yazılımın bir biti dahi değişse üretilen özet çıktısının çok farklı

olmasıdır. Örneğin büyük U ile yazılan Uraz isminin MD5 özet çıktısı "fbc8bf9b15985fc6701ef99e19c7f3e4" iken küçük u ile yazılan uraz isminin MD5 özet çıktısı "b4dca2685b4ed253636ad48638a6baff" olmaktadır. Dolayısıyla 7-zip örneğinden gidersek üreticinin bu yazılımın dağıtımını yaptığı sourceforge.net sitesinde bu yazının kaleme alındığı 28 Mart 2018 tarihinde 7-zip yazılımının son sürümü olan 7z1803.exe için MD5 özet değeri "db573e490e0c5145282aaaf6e2dc34df" iken daha güvenli olan SHA1 özet değeri "1f28fd6afb36e97649d7e534907b13624ed8a645" olarak üreticinin sitesinde kullanıcılara sunulmuştur. Kullanıcılar dosyaları bilgisayarlarına çektikten sonra özet değeri çıkartan yazılımlar ile test yaptıklarında aynı değeri göreceklerdir. Çünkü ne Türk hükümetinin ne de başka bir devletin bu kurulum dosyaları üzerine casus yazılım ekleyip kendi veya başka ülke vatandaşlarına bu dosyaları yönlendirmeleri mümkün değildir. Bunun mümkün olduğunu iddia eden kişinin bakın özetler farklı ben buradan anladım demesi gerekir teknik olmayan adamların kendilerini komik duruma düşürmesi ve suçu MiddleBox varmış işte casusluğun kanıtı demeleri kadar inanılmaz bir iddia ve iftira bulunmamaktadır. Bazen destekli saçmalamak gerekir. Bu iddia hesap makinesine 2+2 yazın 7'ye eşit olduğunu göreceksiniz iddiasından daha saçmadır. Bu yazıyı yeterli görmeyenlerin tek yapması gereken istediği yazılımı indirdikten sonra "file md5 calculator" cümlesini aratmak ve indirdiği dosyaların özetlerini(hash)orijinal üretici sitesinden yayınlanan özetler ile kıyaslamaktır. Sizlerde aynı olduğunu hiçbir kimsenin o kurulum dosyasına 1 bit dahi eklemediğini test ederek görebilirsiniz.

Üçüncü problem ise belki de küreselleşen dünyanın en büyük siber sorunlarından bir tanesi olan Siber Terör eylemleridir. Elbette bahsettiğim konu Wikileaks ve Anonymous gibi büyük korsanlık faaliyetleriyle devletlerin tüm sırlarının ifşa edilmesidir. Burada kişinin kendisine şu soruyu sorması gerekir gerçekten Derin Veri Analizi (DPI) cihazları ile ülkeler casusluk yapılıyor olsaydı bu gerçeği siyaset bilimi profesörlerinden çok siber teröristler ortaya çıkartmaz mıydı? Aslında bu varsayım dahi ülkemize ne kadar büyük bir iftira atıldığını anlatmaya yeter. Bu iftirayı atanlar çokta güzel Türkçe yazabiliyorlar zira bahsi geçen site içinde Türkçe özette koymuşlar. Aynen şöyle yazmışlar "Bu programların resmî web siteleri HTTPS bağlantıyı desteklemelerine rağmen, kullanıcıyı yönlendirdikleri indirme bağlantısı HTTPS olmadığından casus yazılıma yöneltme mümkün olabiliyor." Maalesef 7-zip programının sitesi HTTPS'li https://www.7-zip.org/ ve indirme sitesi de HTTPS'li https://sourceforge.net/projects/sevenzip/files/7-Zip/18.03/.

Anlatmaya çalıştığım verdikleri örnek ile gerçek dünya da birbirini sağlamıyor, bu raporu okuyan insanları bir yalana inanmalarını sağlamaya çalışıyorlar. İşte bilimsel ve teknik bakış açısı burada devreye giriyor, bilim deney ve gözlem demektir. Önemli olan nokta başkalarının ağzından çıkan ifadelere körü körüne inanmak ve bağlanmak değil iddiaları teknik ve bilimsel olarak ele alarak deney-gözlem yaparak sonuca varmak olmalıdır. Batılı bir toplumda bilimsel dayanağı olmayan iddiaların olduğu bir siteyi ve Twitter adresini 40 bin kişi takip ediyorsa bu takipçilerin yüz de kaçı gerçek kişi yüz de kaç troll, bu güzel Türkçe yazabilen kişiler kimler bunu da takdirlerinize bırakıyorum.

Dördündü problem ise herkes tarafından kullanılan en geçerli yöntem olan virüs koruma yazılımları ve güvenlik duvarı yazılımlarıdır, biraz farkındalık sahibi herkes evinde ve/veya işyerinde bu tür yazılımlar kullanıyor. Bahsi geçen raporun içerisinde şöyle bir ifade var "Türkiye'deki enjeksiyonun operatörleri, StrongPity casus yazılımına geçmeden önce, "yasal dinleme" casus yazılımı FinFisher kullanıyordu." Dolayısıyla casus yazılımlar özel olarak Türk Hükümeti tarafından geliştirilmemiş aksine dünyaya mal olan ve çok bilinen yazılımlar olduğu iddia ediliyor. Başka bir ifade ile bu yazılımlar yeni ortaya çıkmadıkları için tüm anti-virüs programlarının bunları algılama kapasitesi olması gerekir, bırakın böyle bir casus yazılımı bilgisayara kurmayı başka bir uygulamaya entegre edilmiş casus yazılım bulunan kurulum dosyasını bilgisayara indirdiğiniz anda bu dosya virüs içeriyor silinecek uyarısını görmeniz gerekir. Tabi bu komplo teorisine dünyanın tüm güvenlik şirketlerini katarsak mesela McAfee, Eset, Kaspersky, BitDefender vs. yani Rusya'dan İsrail'e, ABD'den Çin'e kadar tüm güvenlik sistemlerinin ve şirketlerinin kontrolü Türk Hükümeti'nde derseniz orası başka. Aynı konunun diğer sorunu ise güvenlik duvarları ile bilgisayarınızın dış dünya da nerelerle haberleşebileceğini anlayabiliyor, trafiğe izin verme yada engelleme aktivitelerini gerçekleştirebiliyor olmanız. Bir diğer ifadeyle bir casus yazılım sizin bilgilerinizi dış dünyaya aktaracaksa o da aynı ağ geçidini yani bilgisayarınızın Ethernet yada Wi-Fi ara-yüzünü kullanacağı için güvenlik duvarlarının sizi sayısız kereler uyarması gerekir. Bu iddianın ne kadar saçma olduğunu anlamak için sizde FinFisher Eset yazarak veya FinFisher Kaspersky yazarak arama yaptığınız da bu raporun yayınlanmasından 1 yıl önce bu casus yazılımlar hakkında anti-virüs şirketlerinin koruma bültenleri olduğunu görebilirsiniz.

Teknik raporun sonraki bölümlerinde ilk dikkat çeken husus referansların olmaması, akademik dünyada teknik bir rapor hazırlıyorsanız bazı savlar ortaya atarsınız ancak bu savlardan önce sizi bu bakış açısına sevk eden süreci değerlendirmek için savlarınızı destekler nitelikte literatür dediğimiz diğer akademik kaynaklardan alıntılar verirsiniz örneğin: IEEE, ACM, İnternet, Haber Siteleri vs. yerlerden bir kaynakça tesis eder bu kaynakçadan yazınız içerisine atıflarda bulunursunuz. Teknik rapor da şöyle ifadeler var "Sandvine cihazlarının, Türkiye, Suriye ve Mısır'daki kullanıcıların trafiğine el altından kötü amaçlı ve şaibeli yönlendirmeler enjekte etmesi, ciddi boyutlarda hak ihlali endişeleri doğuruyor.", "Geniş çaplı araştırmamız sonucunda Türkiye ve Mısır'daki yazılım enjeksiyonunun özelliklerini Sandvine PacketLogic cihazlarının özellikleri ile eşleştirdik." vb. Görüldüğü üzere bahsi geçen çok sayıda iddia ve araştırma sonucu rapor içerisine konulmuş ancak bunların nasıl elde edildiği veya nerede yayınlandığıyla ilgili tek bir kaynak dahi konulmamış bir diğer ifadeyle hayal gücüyle yazılmış intiba oluşuyor. Bilimsel tek bir kelimesi olmayan baştan aşağı kadar üzülerek söylüyorum arka planda Türk kökenli yabancılarında olduğuna inandığım bir yazı olmuş. Ben Türkiye'de bir akademisyen olarak başkasının düşüncesini tırnaklar içine alarak veriyorsam bu raporu yazan kişilerinde yüksek akademik kabiliyette kişiler oldukları göründüğünden böylesine basit bir kuralı dahi atladıklarını görünce üzülüyorum.

Ama kuşkucu tavrıma devam ederek yazıyı cımbızlamadan bir bütün olarak ele almam gerektiğine inandığımdan Sandvine Packet Logic cihazlarıyla devam ediyorum. İddia öyle ki Türkiye bu cihazlardan çok sayıda satın almış. Dediklerine göre cihaz üreticisi ABD merkezli ve Kanada merkezli iki firmadan oluşuyormuş. Raporun belki de en bomba cümlesi geliyor "Geliştirdiğimiz Sandvine PacketLogic parmak iziyle eşleşen cihazların, Mısır ve Türkiye'de, internetteki siyasi içeriğin, insan haklarına dair içeriklerin ve haber içeriğinin engellenmesi amacıyla kullanıldığını da tespit ettik." Bu cümleyi analiz etmek için öncelikle parmak izinin ne olduğunu anlamak gerekir. En basit haliyle bir cihaz üzerinden geçen bilgiye üzerinden geçtiği cihaza ait bir bilginin eklenmesi olarak tanımlayabiliriz. Çalışma konularım tam olarak ağ cihazları değil, çalışmalarımda siber güvenliğin bir parçası olarak ağ cihazlarıyla ilgileniyorum. Bu nedenle birden fazla ağ kitabına baktıktan ve araştırma yaptıktan sonra şu kadarını söyleyebilirim TCP paketleri üzerinden geçtiği sayısız ağ cihazına ait parmak izi bilgilerini tutuyor olsaydı TCP paketi içinde asıl iletişim verisinin saklanabileceği yer kalmazdı. Örneğin; G-Mail den e-postalarınıza

bakıyorsunuz, e-postanızı size ulaştıran TCP paketi ABD'den geliyor ve arada 20-30 kadar ağ cihazına uğruyor, bütün bu cihazların üzerinden geçerken hepsine özel parmak izinin TCP paketinize eklendiğini hayal ettiğinizde bunun teknik anlamda boş olduğunu görürsünüz isterseniz kendinizde TCP paketlerinizi WireShark benzeri programlar ile görüntülemeye çalışarak teknik açıdan neden mümkün olmadığını örnekleyebilirsiniz.

Citizen Lab tarafından oynanmış sonuçları elde etme yada yeniden canlandırma imkanınız da bulunmuyor. Bilim de en önemli unsur başkalarının da sizin yönteminizi ve veri setinizi çıkarttığınız mantığı kullanarak aynı sonuca erişebilmesidir. Bu senaryolara ait sonuçlar sadece Citizen Lab çalışma grubuna özel çıktılar olarak kalmaktadır. Anlaşılacağı üzere problemi üreten kendileri, açık bir şekilde yayınlamadıkları veri setini oluşturan kendileri ve çözen yine kendileri olmaktadır. Aynı zaman da senaryolarını desteklemek için Citizen Lab kimsenin aklına gelmeyeni yapmış ve ikinci el bir Sandvine Packet Logic cihazı satın almış hatta rapor içine resmini de eklemiş. Nasıl ele geçirildiği belli olmayan, içine müdahale yapılıp yapılmadığı belli olmayan cihaz üzerinden cihaz parmak izi çıkarttıklarını ve bunun da diğer ülkelerden elde edilen paket içerikleriyle uyumlu olduğunu iddia ediyorlar. Bir diğer ifadeyle başka bir çıkmaz yola insanları sevk ederek teknikten ve bilimden uzak söylemler ile kamuoyu yaratarak Türkiye'yi karalama ve komşularıyla arasına fitne sokma kampanyasına bir tuğla daha ekliyorlar.

Ve sayısız safsata, iftira ve yalan iddialar gerçek dışı varsayımlar ile sürüp gidiyor.

Son olarak Bill Marczak'ın Linkedin sayfasına göre 2005-2009 yılları arasında Pennsylvania Üniversitesi'nden lisans derecesi aldığına değinmeden edemeyeceğim.

Dr. Uraz YAVANOĞLU