Gürkan Caner Birer *Bilgisayar Mühendisi*

>>>

Firmaları Bekleyen Büyük Tehlike

Karanlıknet

Wikileaks, NSA belgeleri, Meksika vatandaşlarının kişisel bilgilerinin internetten yayımlanması gibi olaylar dikkatleri bilgi sızıntılarına çevirdi. Geçtiğimiz aylarda da Türk vatandaşlarının kimlik bilgilerinin internette yayımlanmış olması tepki toplamış ve konuyla ilgili soruşturma başlatılmıştı. Ancak bu durumlarda genelde hedef kamu kurumları ya da kamuya ait bilgilerdi. Panama Belgeleri gibi sızıntılarsa özel firmaların da hedefte olduğunu gösterdi. Üstelik bu bilgiler de birçok kişinin hayatını etkileyebiliyor. Yaşanan olaylar ışığında gelecekte veri sızıntılarının firmalar için çok daha büyük tehditler oluşturacağı söylenebilir.

Kişilerin gerçek kimliklerinin gizlendiği ve internette bıraktıkları dijital izlerin takip edilemediği internet alanları karanlıknet olarak ifade ediliyor. Sıradan bir kullanıcının internette yaptığı her eylem dijital bir iz bırakır. İz bırakmadan hareket edebilmek için güvenlik konularında uzman olmak gerekir. Tor ağı ve Bitcoin gibi son yıllarda ortaya çıkan bazı yazılım ve teknolojilerse, sıradan kullanıcıların da internette iz bırakmadan hareket etmesini sağlıyor. Bu durum kişisel verilerin gizliliği, erişim yasaklarının aşılması gibi iyi niyetli amaçlara hizmet ettiği gibi yasadışı eylemleri gizlemek için de kullanılabiliyor.

Karanlıknetteki sosyal pazar alanlarında kimliği belirsiz kişiler tarafından çeşitli ürünler, bilgiler ve hizmetler satışa çıkarılıyor. Devletlerin güvenlik güçleri bu tür sanal pazar alanlarına yönelik çeşitli operasyonlar gerçekleştiriyor. Ancak bu operasyonlar çoğunlukla yasadışı ürün ve hizmet satışına yönelik oluyor. Özel firmalara ait gizli bilgi ve belgelerin bu gibi alanlarda satışa çıkarılması konusunda yapılabilecekler se hayli sınırlı. Bitcoin gibi dijital para birimlerinin, kimlik gizleyerek satış yapmayı çok daha kolay hale getirmesi, gizli bilgi satışını hızla yaygınlaştırıyor.

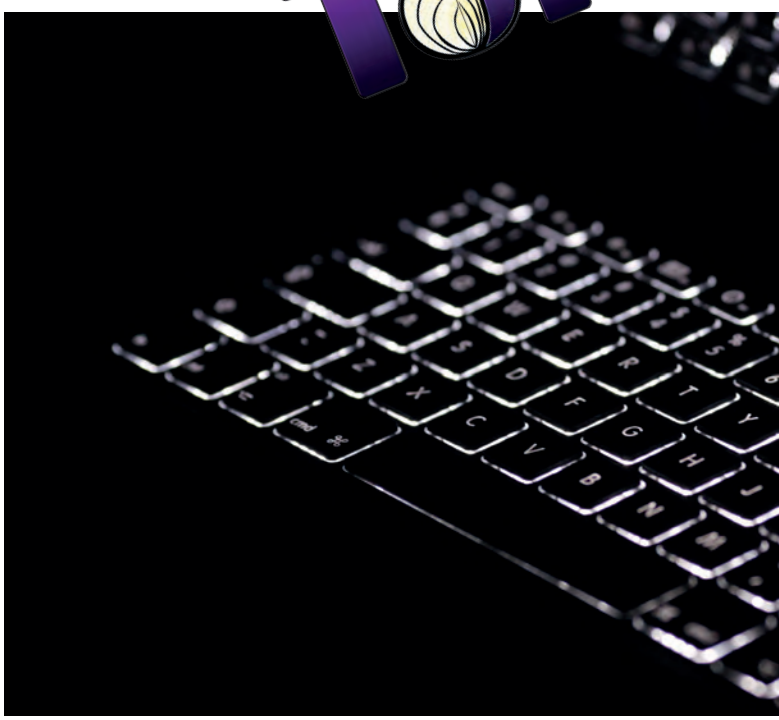
Tor Nedir?

Sıradan insanların gizlilik ve güvenlik ihtiyaçlarını karşılamak için kullandığı, dünya genelinde binlerce gönüllü tarafından işletilen bilgisayarlardan oluşan bir ağdır. Kullanıcılar erişmek istedikleri alana doğrudan bağlanmak yerine, Tor ağını kullanarak bir dizi sanal tünel aracılığı ile bağlanır. Bu sayede hem kişisel bilgilerini, hem de nereye eriştiklerini gizlerler. Ayrıca bulundukları yerden erişime kapalı olan web sitelerine de ulaşabilirler.

Tor ağı, soruşturmalarını gizlemek isteyen savcılardan, haber kaynaklarını açık etmeden dosya hazırlamak isteyen gazetecilere kadar çok geniş bir kitle tarafından kullanılmaktadır.

The Onion Router (Soğan Yönlendirici) anlamına gelen TOR, verileri tıpkı bir soğanın katmanları gibi kat kat şifreler ve ağdaki bilgisayarlara iletir. Her bilgisayar en dıştaki katmanı şifresini çözerek açar ve geriye kalan şifreli veriyi ileteceği bir sonraki bilgisayarın verilerine ulaşır. Şifreli olarak tutulan diğer katmanlar bir sonraki bilgisayara iletilir ve çekirdeğe ulaşana kadar süreç devam eder. Veri çekirdekten hedefe teslim edilir. Kurulan bu tünel üzerinden erişim çift yönlü olarak sağlanır.

Tüm güvenlik yöntemlerinde olduğu gibi Tor da %100 gizlilik sağlamaz. Geçmişte Tor yazılımındaki hatalardan dolayı ağın sağladığı gizlilik devre dışı bırakılabilmişti.



Analizler finans, ilaç ve sağlık sektörlerinin mevcut durumdan en çok zarar gören sektörlerin başında geldiğini gösteriyor. Borsaya açık firmaların hisse değerlerindeki değişimlerle ilgili bilgilerin sızdırılması suretiyle haksız kazanç elde edilmesi, borsa için öteden beri önemli bir tehdit oluşturuyor. Günümüzde borsa işlemlerinde saniyeler hatta milisaniyeler bile önemliyken, karanlıknet değerli bilgilerin sızdırılmasının kolayca ve korkusuzca yapılmasını sağlıyor. İşi daha ilginç ve tehlikeli kılan bir başka etmense yasadışı bilgi paylaşanların yarısının bu işi işvereninden nefret ettiği için yapıyor olması. Karanlıknette, çalıştığı firmanın gizli sunucularına erişim hakkı olup buraya virüs benzeri zararlı yazılım yükleme teklifinde bulunanlar bile var. Firmalara ait bilgi sızdırma faaliyetleri yıllardır sürdüğü halde durumdan habersiz olan firmaların sayısı azımsanmayacak düzeyde.

Firmaları tehdit eden sadece gizli bilgileri paylaşan çalışanlar değil. Karanlıknette hedef gösterilen firmalardan bilgi sızdırma işleri için açık artırmalar yapılıyor. Bu gibi işlemlerde, yeterli teknik bilgiye sahip olmayan ama işini yapmak için gizli bilgilere erişebilen firma çalışanları hedef gösteriliyor ve bu kişiler kullanılarak firmalardan bilgi sızdırılabileceği belirtiliyor. Sonrasında kötü niyetli bilgisayar korsanları, çeşitli teknik ve sosyal mühendislik yöntemleri ile hedef aldıkları bu kişileri istedikleri bilgilere erişmek için kullanıyor. Yapılan analizler hedefteki kişilerin sadece %15'inin firmada liderlik pozisyonunda ya da teknik pozisyonda çalışan kişiler olduğunu gösteriyor. Geriye kalanlar büyük oranda sıradan çalışanlar. Dolayısıyla bilgisayar korsanlarının hedef seçerken dikkat ettiği asıl ölçüt, kişinin pozisyonu değil hangi bilgilere erişebildiğidir.

Veri sızıntısı sadece firmaları değil, firmaların müşterilerini de etkiliyor. Bankalardan, telekomünikasyon firmalarından hatta hastanelerden elde edilen şahıslara ait gizli bilgiler, bu şahıslara zarar vermek için kullanılıyor. Kimi zaman bu bilgilerin nereden, nasıl elde edildiği de ortaya çıkarılamıyor. Sürekli olarak adına hesaplar açılan, banka hesaplarına el koyulan, ilgilisi olmayan faturalarla karşı karşıya kalan kişilerin hayatları mahvolabiliyor.

Firmaların bu gibi tehditlerle mücadele etmesi karmaşık önlemler gerektiriyor. Öncelikle hassas verilere erişimi, bu verilerin taşınmasını ve farklı bir alanda depolanmasını izleyen ve engelleyen DLP (*Data Loss Prevention*) yazılımlarının kullanılması tavsiye ediliyor. DLP yazılımları belirli ölçüde güvenlik sağlasa da yeterli olamıyor. Veri sızıntılarının tespiti ve önlenmesi için daha karmaşık sistemler de kullanılabiliyor. Örneğin karanlıknetteki bilgi paylaşımlarını izleyen ve firmayı ilgilendiren bir durum söz konusu olduğunu fark ettiğinde hemen firmadaki ilgili kişileri bilgilendiren yazılım hizmetleri var. Çalışan bilgilerini analiz edip şüpheli olabilecek kişileri tespit eden makine öğrenme yazılımları da kullanılabiliyor. Ancak bu gibi yöntemlerin ne kadar etkili olduğu tartışmalı bir konu. Teknik önlemlerin yanı sıra çalışanların çalışma şartlarının iyileştirilerek firmaya olan bağlılıklarının ve sadakatlerinin artırılması gibi insani önlemlerin de alınması gerekiyor.

Karanlıknete sızdırılan bilgilerle ilgili bazı rakamlar

- Veri sızıntılarının %43'ünde içerden kişiler kullanılmış. Bu kişilerin yarısı bu işi farkında olmadan yapmış.
- Veri sızıntılarının %40'ı için fiziksel depolama aygıtları -USB bellek gibi- kullanılmış.
- DLP yazılımlarının kullanımı veri sızıntılarının %64'ünü engelleyebilirdi.
- Veri sızıntılarının %32'si şifreli verilerden oluşuyor.
- Sızdırılan verilerin %62'si çalışanların ve müşterilerin kişisel bilgilerinden oluşuyor.
- Verileri sızdırılan firmaların %80'i haftalarca sızıntının farkına varmıyor.

Tüm bu bilgiler ışığında değerlendirildiğinde verilerin korunması, sızıntıların engellenmesi konusunun firmalar için öneminin her geçen gün arttığı görülüyor.

XXX telefon operatöründe çalışıp da SIM değiştirme işlemi yapabilecekler benimle iletişime geçsin, ücret ödenecektir.

Örnek bir karanlıknet mesajı.

Kötü niyetli bir kişi, bir telefon operatörü firmasında çalışan birisini kullanarak, hedefteki kişinin SIM kartını değiştirip -sosyal medyada yer alan bilgileri de kullanarak- banka hesabına ulaşabilir.
Böylece bir hesaptaki parayı başka hesaplara transfer edebilir. Çoğunlukla mağdur olan kişinin durumu fark edip de yetkililere durumu bildirmesi ve konuyla ilgili bir işlem başlatılması günler alır.

Kaynaklar: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ - http://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf