14 Ağustos 2016, Pazar

MAHMUT ÖVÜR

Nereler siber saldırının hedefi?

Türkiye, 7 Şubat 2012 MİT Operasyonundan bu yana içeriden ve dışarıdan yoğun bir saldırı altında. Biri bitmeden öteki başlıyor.

Bırakın iç ve dış siyaset odaklarını, FETÖ dahil DAEŞ, PKK ve DHKP-C gibi irili ufaklı bütün terör örgütleri Türkiye'ye saldırıyor.

15 Temmuz işgal hareketi bu topyekun saldırının en hayasız olanıydı.

Ancak, Türkiye toplumunun destanlaşan direnişiyle bu hayasız saldırı püskürtülmesine rağmen durmayacak gibi... Daha üzerinden bir hafta geçmeden PKK kanlı eylemlerini başlattı. Büyük olasılıkla DAEŞ de yakında harekete geçer.

Peki, kanlı darbeye imza atan FETÖ ne yapar?

FETO, hem devletin kılcal damarlarına kadar sızan hem de küresel desteği olan tehlikeli bir örgüt. Bu nedenle şu sıralarda ne yapacağı daha çok merak ediliyor.

Halkı ve Meclis'i bombalayacak kadar vahşileşebilen bu yapı, son teknolojiyi de iyi kullanıyor.

FETÖ'nün intihar saldırılarından, toplumu birbirine kırdırmaya kadar uzanan birçok eylemi yapabileceği biliniyor ama en çok üstünde durulan ve beklenen **"siber saldırı"** eylemi.

Yani kaybettiği için çılgınlaşmakta sınır tanımayan FETÖ'cülerin, ülkenin teknolojik altyapısını yıkmakta hiç tereddüt etmeyecekleri söyleniyor.

O teknolojik alt yapıların neler olduğunun cevabını ise Türkiye'nin dünya çapında teknoloji üreten firması Natek Yönetim Kurulu Başkanı **Tolga Erpolat** veriyor:

"Siber saldırının hedefi ülkemizin kritik altyapılarıdır. Enerji, finans, sağlık, savunma, ulaşım ve bilişim önemli kritik altyapılardır."

Peki, neler yapabilirler?

Erpolat'a göre en kolay ve zahmetsiz olanı **"Servis dışı bırakma (DDoS) saldırılarıdır."** Yani ülkenin bilişim ana servis sağlayıcı merkezini devre dışı bırakmak. Bunun örneğini geçen yıl 14-17 Aralık 2015 tarihinde yaşadık. **O saldırıda ODTÜ'de bulunan ana DNS (Domain name sever)'ler yavaşlamış ve birçok kurumumuz hizmet veremez hale gelmişti**. Bankalar ve diğer finans kuruluşları bu saldırı

nedeniyle milyon dolarlarla ifade edilen zarar yaşadı. Elektrik ve sağlık sistemi de benzer biçimde devre dışı bırakılabilir.

İkinci önemli saldırı alanı ise **savunma**... Bu konuda da ses trafiğinin dinlenmesi, trafiğin arasına girerek yanlış yönlendirme yapılması, planların ele geçirilmesi gibi çok stratejik risklerden söz ediliyor.

Erpolat saldırıların nereden geleceği konusunda da şunları söylüyor:

"Bu saldırılar sadece dışarıdan değil içeriden de yapılabilir. İç ağımızda oluşturulmuş arka kapılar (back door) veya zararlı yazılımlar (malware, virüs vb.) ile de bu servis dışı bırakma saldırısı gerçekleştirilebilir. Görevden almaların yoğun yaşandığı bu süreçte kişilerin bu tarz açık kapılar bıraktığı ihtimali üzerinde durmak gerekir."

"Milli ve yerli yazalım"

Gelelim alınması gereken acil önlemlere... Teknik ayrıntıya girmeden **Erpolat**'ın şu tespitini aktaralım:

"En önemli tedbir, tüm sistemlerimizde ya da en azından kritik sistemlerimizde zararlı yazılım analizi yaparak gerekli temizliği gerçekleştirmek... Ancak bu yetmez. Tüm kritik organizasyonların altyapısını oluşturan bilişim sistemlerinde çoğunlukla yabancı menşeli ürün kullanılması aslında risk katsayımızı artırmaktadır. Çünkü **bu sistemlerin içerisine üreticiler açık kapı bırakabilirler ve cihazları bir anda zombi ordusuna dönüştürebilirler. Bu noktada milli çözümlerin kullanılması ve milli üreticinin desteklenmesi gerekiyor.**"

Ve önemli bir uyarı: Bilgi işlem birimlerinde 7/24 esasına göre nöbetleşe çalışılması ve tüm ağ trafiğinin incelenmesi gerekmektedir. Ülkemizin merkezi DNS'lerini yöneten kuruma ve internet servis sağlayıcılarımıza büyük görev düşmektedir.

YAZARIN ÖNCEKİ YAZILARI Tüm Yazıları >

- **'Altın nesil'den katil çıkarmak (13.8.2016)**
- **Gladyo, MİT ve FETÖ (12.8.2016)**
- **Yenikapı'nın asıl mesajı, ABD ve AB'ye (8.8.2016)**


SABAH