İÇİNDEKİLER

24 SAAT

Yayın Adı	: 24 Saat Gazetesi	Yayın Tarihi	: 23.02.2015	Küpür Sayfa	: 10
Referans No	: 45376745	Etki	: Etkisiz	Tiraj	: 1250
Renk	: Renkli	STxCM	: 183,055555	Sayfa	: 10

Türkiye'de istenmeyen e-posta oranı yüzde 140 arttı

20 ülkede 3500'den fazla kurum ve kuruluşun güvenliğini sağlayan Labris Networks, siber güvenlik raporunu açıkladı. 2014 yılı boyunca yapılan incelemelerde Türkiye'de özellikle spam konusunda önemli sorunların yaşandığı ortaya çıktı. İletilen tüm e-postalarda spam oranının %84'e ulaştığının belirtildiği raporda, tehditlerin ürettiği alarmların da bir önceki yıla göre %10 oranında bir artış gösterdiği vurgulanıyor. 2014 yılında casusluk ve fidye amaçlı kullanılan kötücül yazılımların zirve yaptığını ortaya koyan rapor siber dünyanın da artık bir savaş alanı olduğunun altını çiziyor.

HABER MERKEZİ- 2003 yılında Türkiye'nin ilk ticari ulusal güvenlik duvarını, 2005 yılında Türkiye'nin ilk yerli UTM ürününü geliştiren ve bünyesinde kurduğu SOC (Security Operations Center) merkezinde siber dünyayı 7/24 anlık takip ve kontrol edebilen Labris Networks, 2014 Siber Güvenlik Raporunu ve 2015 Öngörülerini açıkladı.

Labris SOC'den elde edilen verilerle oluşturulan raporda Türkiye özelinde ve tüm dünya genelinde yaşanan olaylar derleniyor. 2014 yılı boyunca yapılan incelemelerde Türkiye'de özellikle spam konusunda önemli sorunların yaşandığı ortaya çıktı. İletilen tüm e-postalarda istenmeyen eposta oranının %84'e ulaştığının belirtildiği raporda, spam e-posta miktarının bir önceki seneye göre %140 arttığı da ortaya kondu. İstenmeyen e-postalarda en çok karşılaşılan konunun online ürün satışları olduğu söylenirken, yeni yürürlüğe giren e-ticaret kanunu ile spam e-posta miktarının azalabileceği de belirtildi. İstenmeyen e-postalarda online ürün satışlarını sırasıyla, kötücül yazılım taşıyan iletiler, kurumsal teklifler, arkadaşlık ağları ve cinsel içerikli e-postalar takip ediyor.

2014 boyunca Labris SOC'da gözlenen kişisel bilgisayar tabanlı kötücül yazılımların %96'sının Windows platformunu hedef aldığı, mobil tabanlı kötücül yazılımların ise %97'sinin Android platformunu hedeflediği bilgisi de raporda yer alıyor. Tehditlerin ürettiği alarmların da bir önceki yıla göre %10 oranında bir artış gösterdiği vurgulanıyor.

2014 ŞANTAJ VE CASUSLUK YILI

Labris Networks tarafından hazırlanan rapor, 2014 yılında casusluk ve fidye amaçlı kullanılan kötücül yazılımların zirve yaptığını ortaya koydu. E-posta ve web üzerinden yayılan fidye amaçlı kötücül yazılımlar kullanıcıların dosyalarını şifreleme, hesaplarını ele geçirme gibi işlemler için kullanılabiliyor. Bu yazılımları kontrol eden kişiler daha sonra şifreleri kaldırmak için para talebinde bulunuyor. ABD başta olmak üzere tüm dünyada etkili olan Crypto Locker, 2014 yılında fidye amaçlı kullanılan kötücül yazılımların en önemli örneği oldu.

2014'te adını en çok duyuran casus yazılımlar ise Caredo ve Reign'di. Özellikle Caredo, başta Fas olmak üzere Kuzey Afrika ülkelerinde diplomatik ve hükümete ait merkezleri hedef alarak önemli zararlar verdi. Bunun yanı sıra Belgacom'un hack'lenmesi, Doğu Avrupa ülkelerinde etkili olan ve Rusya'nın arkasında olduğu iddia edilen APT28 ve Çin destekli olduğu belirtilen Operation SMN gibi espiyonaj kampanyaları, kötücül yazılımların kullanıldığı öne çıkan olaylar arasında yer aldı. 2014 yılında yaşanan bu olaylarla birlikte siber casusluğun artık normalleştiği yorumunun yapıldığı raporda, ABD ve İngiltere gibi ülkelerin artık bu duruma karşı güçlerini birleştirme kararı aldığından da bahsedildi.

TARİHİN EN BÜYÜK DDOS SALDIRISI

Labris Networks'ün hazırladığı detaylı rapora göre 2014 yılı tarihin en büyük DDoS saldırısına sahne oldu. Kasım ayında düzenlenen 500 Gbps büyüklüğündeki saldırı kayıtlara en büyük DDoS saldırısı olarak geçti. DDoS saldırılarının yanında son kullanıcıların kişisel verilerini sızdırmaya yönelik çok sayıda saldırı da 2014 yılının gündemine oturdu. Milyonlarca kullanıcısı olan servislerin ele geçirilmesi sonucunda kişisel dosyalar ve hesaplara ait bilgiler ele geçirildi. Yapılan bazı saldırıların arkasında ülkelerin olduğu iddiaları ise uluslararası krizlere yol açtı.Kara, deniz ve havadan sonra siber dünyayı da bir savaş alanı olacağını geçmişte belirtmiş olan ABD, Son saldırısı ile bu anlamda en belirgin örnekler-den birine maruz kaldı. Labris Networks 2014 Siber Güvenlik Raporu'na göre geçtiğimiz yıl sorun yaşanan alanlar arasında açık kaynaklı yazılımlar da yer aldı. Özellikle OpenSSL platformunda ortaya çıkan Heartbleed adlı açık SSL sunucularından kişisel verilerin sızdırılmasına yol açtı.

2015'TE BİZLERİ NELER BEKLİYOR

20 ülkede 3500'den fazla kurum ve kuruluşun güvenliğini sağlayan, tüm dünyada Ortak Kriterler EAL4+ sertifikasına sahip 12 şirketten biri olan Labris Networks tarafından hazırlanan raporda 2015 yılına dair öngörüler de paylaşıldı.

2015 yılında kötücül yazılım hazırlamanın çok daha kolay hale geleceği yönünde uyarılarda bulunan Labris Networks, siber suçluların kötücül yazılımlar için yapım kitleri ve kılavuzları çıkarmaya başladığını ve artık temel bazı bilgilere sahip olan birçok kişinin rahatlıkla spesifik amaçlara yönelik saldırılar yapabileceğini belirtti.

Kişisel bilgisayar kullanımının yerini artık mobil cihazlara bıraktığı bu dönemde şimdiye kadar sadece mobil cihazları hedef alan büyük saldırılar olmadığına dikkat çekilen raporda mobilde de şantaj amaçlı kullanılan yazılımların daha sık karşımıza çıkacağı belirtiliyor. Son dönemde popüler olan "Nesnelerin İnterneti" (IoT) konseptinin de güvenlik sorunlarını beraberinde getirdiğini belirten Labris Networks, akıllı televizyon, otomobil, saat, bileklik gibi cihazlara yönelik saldırıların da olabileceğini söylüyor.

Keşfedilen açıklar nedeniyle büyük zararlar yaşatan açık kaynak kodlu yazılımlara güvenin sarsıldığının belirtildiği raporda sık kullanılan bu tip yazılım ve protokollere saldırıların devam edeceği öngörülüyor.

Harpp DDoS Mitigator siber savaş ürün ailesiyle DDoS saldırılarına karşı güvenlik sağlayan Labris Networks, 2015'te DDoS saldırılarının çok daha kompleks hale geleceğini, birçok kurumun mevcut koruma sistemlerinin ve ISP tabanlı koruma önlemlerinin, gittikçe akıllanan DDoS saldırılarına karşı koyacak güçte olmadığını belirtiyor.

Labris Networks tarafından hazırlanan rapor, kamu, askeri ve özel kuruluşların tamamının riskler karşısında farkındalığını artırmayı hedefliyor. Güvenlik risklerine karşı çözümlerin yalnızca ürün değil; ürün, hizmetler ve bilginin bütünleşik olarak kullanılmasını gerektirdiğini belirten Labris Networks, bu üçlünün güvenliği, kurumların iş verimliliğini artırırken