İÇİNDEKİLER

BThaber

Yayın Adı	: BT Haber	Yayın Tarihi	: 16.03.2015	Küpür Sayfa	: 1
Referans No	: 46017679	Etki	: Etkisiz	Tiraj	: 7500
Renk	: Renkli	STxCM	: 7,500000	Sayfa	: 1

Oğuz Yılmaz

Kötücül yazılımlar zirve yaptı

SOC merkezinde siber dünyayı 7/24 anlık takip ve kontrol eden Labris Networks, 2014 Siber Güvenlik Raporu'nu ve 2015 öngörülerini açıkladı.

BTHaber

Yayın Adı	: BT Haber	Yayın Tarihi	: 16.03.2015	Küpür Sayfa	: 25
Referans No	: 46017679	Etki	: Etkisiz	Tiraj	: 7500
Renk	: Renkli	STxCM	: 7,500000	Sayfa	: 1

2014'te kötücül yazılımlar zirve yaptı

Sedef Özkan

Bünyesinde kurduğu SOC (Security Operations Center) merkezinde siber dünyayı 7/24 anlık takip ve kontrol eden Labris Networks, 2014 Siber Güvenlik Raporu'nu ve 2015 öngörülerini açıkladı. Rapora göre; 2014 yılı tarihin en büyük DDoS saldırısına sahne oldu.

Labris Networks CTO'su Oğuz Yılmaz

Labris Networks CTO'su Oğuz Yılmaz, Güvenlik Raporu ile bağlantılı olarak 2014 yılında güvenlik tehditlerinin çeşitlendiğini vurgulayarak özellikle tehditlerin siberin yanında fiziksel ortamları da etkiler hale geldiğini kaydetti. Yılmaz, "Dünya Ekonomik Forumu'nun dünya ekonomisini tehdit eden tehditler sıralamasında 'siber saldırılar' hem etki gücü hem de olasılığı bazında en uçta değerlendiriliyor. Çok büyük bütçelerde dahi tehditlerin realize olabiliyor olmasını ürün bazlı bakışa bağlıyoruz. Kurumlar, artık insan kaynağına ve ürünü en etkin şekilde kullanabilecek ekiplere kıymet vermeli, sistem-süreç bakışını kazanmalı, hem yönlendirebilme olanakları hem de güven yönlerinden yakın olabildiği üreticileri tercih etmeliler" yorumunu yaptı.

Siber dünya artık bir savaş alanı

Labris SOC'den elde edilen verilerle oluşturulan Siber Güvenlik Raporu'nda; Türkiye özelinde ve tüm dünya genelinde yaşanan olaylar derleniyor. Rapora göre; 2014 yılı boyunca yapılan incelemelerde Türkiye'de özellikle 'spam' konusunda önemli sorunların yaşandığı ortaya çıktı. İletilen tüm e-postalarda 'spam' oranının yüzde 84'e ulaştığının belirtildiği raporda, tehditlerin ürettiği alarmların da bir önceki yıla göre yüzde 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. Raporda, Türkiye'de 'spam' e-posta miktarının bir önceki seneye göre yüzde 140 arttığı da ortaya kondu. İstenmeyen e-postalarda en çok karşılaşılan konunun çevrimiçi ürün satışları olduğu söylenirken, yeni yürürlüğe giren e-Ticaret Kanunu ile spam e-posta miktarının azalabileceği de belirtildi. İstenmeyen e-postalarda çevrimiçi 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 yüzde 96'sının Windows platformunu hedef aldığı, mobil tabanlı kötücül yazılımların ise yüzde 97'sinin Android platformunu hedeflediği bilgisi de raporda yer alıyor.

Adını en çok duyuran casus yazılımlar: 'Caredo' ve 'Reign'

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 saldırısı, 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.

Saldırılar uluslararası krizlere yol açtı

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 örneklerden 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 mobilde şantaj amaçlı yazılımlar daha sık karşımıza çıkacak!

2015 yılında kötücül yazılım hazırlamanın çok daha kolay hale geleceği yönünde uyarılarda bulunan Labris Networks yetkilileri, 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 internet'inin de (IoT) güvenlik sorunlarını beraberinde getirdiğini belirten Oğuz Yılmaz, 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. 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 optimize etmesinin önemini vurguluyor.