Siber Güvenlik Raporu '14

Ömer Faruk ALTUNDAL

Rapor Hakkında

Bilişim dünyası için zorlu geçen bir yıl oldu. İletişimin temellerinde kullanılan güvenlik protokollerinin sandığımız kadar güvenli olmadığını fark ettiğimiz bir yıl… Ezberleri bozan, üreticilerin kendi uygulamalarından kaynaklanan zafiyetlerin gölgede kaldığı; bunun yerine, defacto standart olarak kullanılan uygulamalarda bulunan açıklıkların keşfedildiği bir dönemden geçtik. Bu açıklıkların halen tamamen giderilmediğini, kalıntılarıyla halen yeni zafiyetlerin keşfedildiğini ve bunları sömürmek için saldırı vektörlerinin geliştirildiğini görmekteyiz.

Bir tarafta güvenlik araştırmacıları yukarıda sayılan güvenli iletişim standartlarını zorlarken, diğer tarafta saldırganlar da alışılagelmiş yöntemlerle sistemlere zarar vermekten geri durmadı. Mobil ve web tabanlı saldırıların yoğunluğunun daha da arttığı 2014'de, kullanıcı bilinçsizliğinin suiistimal edildiği pek çok vaka yaşandı. Ülkemiz de bu tip saldırılardan nasibini fazlasıyla aldı.

2014 özellikle defacto standartların temellerinin sarsıldığı bir yıl oldu

Bu raporda, 2014 senesi boyunca yaşanan ve dünya çapında ya da ülkemizde büyük ses getiren güvenlik olaylarından bahsedilmiştir. Sadece yaşanan güvenlik ihlalleri ve olayları ele alınmamış, aynı zamanda güvenlik ezberlerini bozan çok kritik sistem zafiyetlerinden de bahsedilmiştir. Güvenlik zafiyetleri ve saldırılarla birlikte, vakalara ilişkin istatistikler, trendler ve geleceğe yönelik siber saldırı senaryolarından bahsedilmiştir.

İçindekiler

Güvenlik Olayları/Zafiyetleri

Bu bölümde, 2014 boyunca ortaya çıkan güvenlik zafiyetleri ve gerçekleşen güvenlik vakalarından en çok öne çıkanlar irdelenmiştir.

Zafiyet veya olayların etki alanını göstermek için aşağıdaki simgeleri takip edebilirsiniz;

Bu simge, yaşanan olayın tüm dünyada etki yarattığını göstermektedir.

Yaşanan olayın özellikle Türk firmalarını ya da Türk müşterileri hedef aldığını gösterir.

Belli bir firmanın/grubun hedef alındığı olaylardır. Burada varsa hedefin logosu kullanılmaktadır.

Heartbleed

2014 yılının belki de en çok ses getiren güvenlik olayı – Heartbleed. Google güvenlik araştırmacılarının 2014 Nisan'ında bulduğu bu zafiyetin, bulunduğu tarihte dünya çapında yaklaşık 500.000 web sitesini etkilediği tahmin edilmektedir. Bu da ilgili tarih itibariyle tüm web sitelerinin %17'sine denk gelmekteydi.

Kriptolu iletişimde (SSL/TLS) yaygın olarak kullanılan, açık kaynak kodlu, neredeyse defacto diyebileceğimiz OpenSSL kütüphanelerinde bulunan bu zafiyet nedeniyle, hedef sistemlerde bulunan kritik veriler ele geçirilebilmektedir. Bu kritik verilerin arasında güvenlik sertifikasının anahtarı, kullanıcı isimleri ve parolalar bulunmaktadır.

Zafiyetin ortaya çıktığı tarihte tüm dünyada büyük ses getirmiş ve bilişim camiasında büyük paniğe neden olmuştur. Öyle ki; Google (arama motoru, Gmail vs) Instagram, Yahoo Mail, Amazon, Flickr, YouTube, Tumblr gibi dünya çapında yaygın olarak kullanılan servislerin zafiyetten etkilendiği kesinleşmiş ya da şüphelenilmiştir. Zafiyetin yayınlanmasından, yamaların geçilmesine kadar geçen süre içerisinde bu servisleri kullanan kullanıcıların erişim bilgileri çalınmış olabilir. Güvenlik yamalarını henüz geçmemiş ya da sertifikasını güncellememiş tüm sistemlerin halen bu zafiyetten etkilenme ihtimali bulunmaktadır.

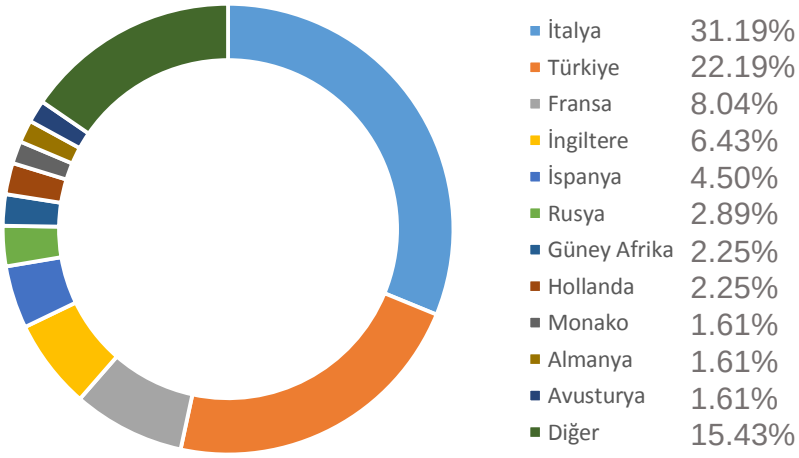
Cryptolocker

Özellikle ülkemizde "Sahte Fatura" gönderimiyle başlayan phishing (oltalama) sürecinin son aşaması olan cryptolocker, çok sayıda kişi ve kurumu maddi zarara uğratmıştır. Türkiye'deki uygulama yolu; sahte fatura gönderimi ile başlamakta, sonrasında yönlendirilen sitedeki zararlı dosyanın çalıştırılmasıyla sisteme bulaşmaktadır.

Ana hedefi, sistemde bulunan Word, Excel, PDF, Imaj, SQL vb dosyaları şifrelemek ve şifrelerin çözülmesi için kurbandan para talep etmektir. Bu nedenle **ransomware** kategorisinde değerlendirilen bu zararlı yazılım tamamen kurban kişilerin bilinçsizliğini hedef almaktadır. İşletim sisteminin shadow copy yedekleri olmadığı durumda, ilgili dosyaların fidye ödenmeden geri getirilmesi neredeyse imkansızdır.

Ülkemizde de son dönemde telekom sektöründe, daha öncesinde de THY gibi kurumlar adına gönderilen sahte e-postalarla çok sayıda kişi ve kurum zarar görmüştür. Bu zararlıdan etkilenen kurbanların tamamından geri dönüş olmaması ve kaybedilen dosyaların finansal boyutu bilinmediğinden, maddi zarar tam olarak hesaplanamamaktadır.

TrendMicro'nun Kasım 2014 araştırmasına göre EMEA bölgesinde Cryptolocker'dan en fazla etkilenen ülkeler şunlardır;



Shellshock

Shellshock da yine Heartbleed gibi neredeyse defacto olarak kullanılan bir uygulamada ortaya çıkan zafiyettir. Yaygın olarak kullanılan, Unix/Linux tabanlı işletim sistemlerinin en popüler kabuk uygulaması olan BASH (Bourne-Again Shell) üzerinde çıkan bu zafiyet dünya çapında milyonlarca sistemi etkiledi. Bu zafiyet kullanılarak hedef sistem üzerinde istenen komutun uzaktan çalıştırılması olanaklı hale gelmiştir. DHCP, HTTP (CGI ile) gibi protokoller ile sistemde oturum dahi açılmadan, ya da sistemde düşük yetkili kullanıcı ile oturum açarak, daha yüksek yetkili kullanıcılar adına işlem yapılması mümkün olmuştur.

2014 Eylül'ünde ifşa olan bu zafiyet; RedHat, Oracle (Solaris ve diğer pek çok uygulama), IBM AIX, F5, Cisco, BlueCoat gibi büyük üreticilerin neredeyse tamamında, ürünlerinin de çoğunda görülmüştür.

Veri Hırsızlığı

2014 senesinin en çok konuşulan olaylarından biri yine veri hırsızlıkları oldu. Dünya çapında pek çok ticari işletme, ticari olmayan kurumlar ve devlet kurumları bu saldırılardan nasibini aldı. Anılmaya değer pek çok vaka olmasına karşın, hacim ve getirdiği ses bakımından en çok öne çıkanlardan bahsedeceğiz.

iCloud… Apple'ın müşterilerine sunduğu ve önemli verilerini saklamalarına imkan veren bir bulut bilişim çözümüdür. Kullanıcılarının cihazlarında bulunan dosyaların bir kopyasının tutulduğu iCloud sistemi 2014 senesi içerisinde saldırıya maruz kaldı. Saldırı sonrasında, içinde Jennifer Lawrence, Kirsten Dunst gibi ünlülerin olduğu kişilerin mahrem fotoğrafları internet ortamında yayıldı. Fotoğrafları yayılan kişilerin sert tepki gösterdiği olayın iCloud kaynaklığı olduğu iddiaları Apple tarafından kesin bir dille yalanlandı. Şirket, olayın sahte bir web sitesi kullanmak yoluyla Man-In-The-Middle adı verilen saldırı tekniği ile kullanıcı hesaplarının ele geçirilmiş olabileceğini öne sürdü.

Yıl içerisinde yaşanan önemli veri hırsızlıklarından birinin kurbanı da Sony Pictures isimli film yapım şirketi oldu. 2011 senesinde, Play Station Network'e yapılan saldırıda, 77 milyon kullanıcı bilgilerinin sızdırıldığı saldırı sonrası, Sony'nin bu kez de film şirketi saldırıya uğradı.

SONY PICTURES

GOP isimli bir hack grubu tarafından üstlenilen saldırıda, Sony Pictures'a ait sunuculardan terabaytlarca dosya indirildi. Bu indirilen dosyaların içerisinde halen gösterimde olan ve Brad Pitt'in başrolünde olduğu Fury isimli film de vardı. FBI tarafından yapılan araştırma sonucunda, yaşanan olayın arkasında Kuzey Kore'nin parmak izi olduğu duyuruldu. Daha önce de Kuzey Kore liderine yönelik suikasti konu alan komedi filmi nedeniyle, Sony tehditlere maruz kalmıştı. Bu durum da, yaşanan olayın ardında Kuzey Kore olduğu ihtimalini güçlendiriyor.

Veri Hırsızlığı

Yıl içerisinde yaşanan bir diğer veri hırsızlığı haberi ise Amerika'dan geldi. Finans sektörünün köklü kuruluşlarından J.P Morgan Chase, Ekim Ayı içerisinde siber saldırıya uğradığını duyurdu. 76 milyon bireysel müşteriye ait bilgilerin ve 7 milyon kadar küçük ölçekli işletmeye ait bilgilerin sızdırıldığı saldırı sonrası yapılan açıklamada '*herhangi bir finansal bilginin çalınmadığı, bu nedenle parola değişikliği gibi işlemlerin gerekmediği*' belirtildi.

Kurumdan yapılan açıklamada, çalınan bilgilerin isim, adres, telefon numarası ve elektronik posta adresleri gibi müşteri iletişim bilgilerinin olduğu; hesap numarası, parola, doğum tarihi, sosyal güvenlik numarası gibi bilgilerin ele geçirilmediği öne sürüldü. FBI tarafından soruşturulan saldırı olayının aslında ilk olarak Temmuz 2014'de bankanın güvenlik ekibi tarafından tespit edildiği belirtiliyor.

Arkasında Rus hacker gruplarının olduğu sanılan bu siber saldırı, toplamda 83 milyon müşteri bilgisinin sızmasıyla gelmiş geçmiş en büyük siber saldırılardan biri olarak kabul edilmektedir.

2014 senesinin siber saldırı hedeflerinden biri de eBay oldu. Amerikan merkezli olan ve Türkiye'de de gittigidiyor.com'u satın alan online alışveriş sitesi eBay'in hedef olduğu saldırı yine bir veri hırsızlığını amaçlıyordu.

Bu yaşanan olayda sızdırılan verilerin kritikliği J.P Morgan vakasındaki kadar yüksek olmasa da, hacim olarak çok daha yüksek sayıda müşteri verisi ele geçirilmişti. Basına yansıdığı kadarıyla 150 milyon kadar müşterinin kullanıcı bilgileri çalınmıştı. eBay'den yapılan açıklamaya göre çalınan bilgilerin arasında kredi kartı bilgisi gibi finansal bilgiler olmasa da kullanıcıların parolaların değiştirilmesi istendi. Bu yaşanan vaka da bize, en büyük kurumların da ne kadar önlem alsa da siber saldırılara açık olduğunu gösterdi.

Veri Hırsızlığı

Tüm dünyada siber saldırılar sonucu yaşanan veri hırsızlıklarından tabi ki Türk firmaları ve müşterileri de nasibini aldı. Bunun en büyük örneği ise finans sektöründe yaşandı. Hong Kong merkezli İngiliz bankası HSBC'nin Türkiye operasyonu 2014 içerisinde önemli bir siber saldırıya uğradı.

Yaşanan saldırı sırasında 2.7 milyon kadar müşterinin kredi kartı bilgileri ile debit kartı bilgilerinin çalındığı duyuruldu. Saldırıyı üstlenen belli bir grup olmazken, saldırıda müşteri ismi, kart son kullanma tarihi ve hesap numaralarına ulaşıldığı açıklandı. Bankanın yaptığı açıklamaya göre müşteriler herhangi bir finansal risk altında olmamasına karşın, güvenlik camiasında, sızdığı açıklanan bilgilerle sahtecilik işlemleri yapılması riskinin bulunduğu görüşü hakimdir.

Diğer taraftan, Banka'nın hem BDDK'ya bilgilendirme yapması, hem de kamuyu aydınlatıcı şekilde yaşanan vakayı açıklaması yaşanan olaya rağmen şeffaflık açısından takdir toplamıştır.[1]

2014 senesinin bu şekilde kapanacağı beklenirken, bir haber de telekomünikasyon sektöründen geldi. GSM sektöründe faaliyet gösteren Turkcell'in, müşterilerine çevrim-içi destek vermek için kullandığı **TurkcellHizmet** isimli Twitter hesabı **UygurTim** adlı hacker grubu tarafından ele geçirildi.

2014 Aralık ayında yaşanan bu olayla ilgili, Turkcell tarafından '*müşteri bilgilerinin güvende olduğu*' yönünde bir açıklama yapıldı. Turkcell tarafından böyle bir açıklama yapılsa da, bu Twitter hesabı üzerinden Direk Mesaj aracılığıyla müşteri bilgileri alındığı bilinmektedir…

1- HSBC Açıklaması : http://www.hsbc.com.tr/tr/haberler/haber_detay.asp?NewsId=984

POODLE

2014 senesi iletişim standartlarının alt üst olduğu bir yıl olmaya devam etti. Kriptolu iletişim protokollerinden olan Secure Sockets Layer (SSL) üzerinde bir zafiyet daha tespit edildi. SSL'in önceki sürümlerinden farklı olarak, SSL v3 güvenli olarak kabul ediliyor ve 1996'dan beri neredeyse tüm uygulamalarda kullanılıyordu. Ortaya çıkarılan zafiyet ise bu kabulü temelinden yıktı.

Google güvenlik araştırmacıları Bodo Möller, Thai Duong, Krzysztof Kotowicz tarafından keşfedilen bu açık, kriptolu iletişimin arasına girerek trafiğin elde edilmesine imkan vermektedir. **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption – **POODLE** olarak adlandırılan bu zafiyet, keşfedildiği tarihe kadar tüm internet tarayıcılarında, mobil veya web uygulamalarında ve diğer platformlarda kullanılmaktaydı. Bu zafiyeti sömürmek için yapılan saldırıda, ortadaki adam / Man-In-The Middle (MITM) tekniği kullanılmaktadır. Normal şartlarda şifreli trafiğin arasına girilse de okunamayacak veriler, teorik olarak bu zafiyet sayesinde okunabilir hale gelmektedir.

SSL v3'de bulunan bu zafiyetten korunmak için uygulamalarda, internet tarayıcılarında SSL v3 desteğinin iptal edilmesi gerekmektedir. Google ve Mozilla bu zafiyetin yayınlanmasından sonra kısa süre içerisinde Chrome ve Firefox üzerinde SSL v3 desteğini tamamen kaldırmıştır. Her ne kadar firmalar bu desteklerini çekse de halen çok sayıda web sitesi SSL v3 desteği vermekte, bu da kullanıcılarını bu zafiyete karşı açık hale getirmektedir.

Güvenlik şirketi olan Qualys'in hazırladığı https://www.ssllabs.com gibi adresler kullanılarak bir sitenin bu zafiyeti ve daha önceki sayfalarımızda anlattığımız HeartBleed zafiyetinin olup olmadığı test edilerek gerekli önlemler alınabilir.

Peki Ya Sonra?

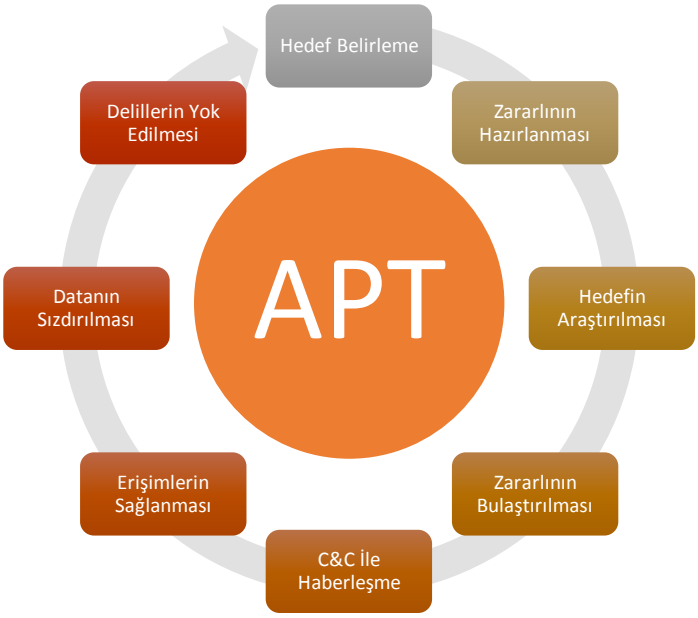
2014 senesi, tüm dünyada siber güvenlik açısından firmaları ve kamu kurumlarını gerçekten çok zorlayıcı bir yıl oldu. Peki bundan sonra ne olacak? Bizleri neler bekliyor?

Bu bölümde, yıl boyunca yaşanan siber olaylardan ve gelişen teknolojiden yola çıkarak, önümüzdeki dönemde ne gibi tehditlerin oluşacağı, siber saldırıların hangi teknolojiye ve hangi hedeflere doğru kayacağı konusunda bir projeksiyon çizeceğiz.

APT

APT – Advanced Persistent Threat, Türkçemizde daha çok Gelişmiş Hedef Odaklı Saldırı olarak ifade edilmektedir. APT terimi ilk olarak Amerikan Hava Kuvvetleri tarafından 2006 yılında; karmaşık, belli bir hedefe yönelmiş olan ve uzun süreli devam eden tehditler için kullanılmıştır. Her ne kadar askeri bir terim olarak ortaya çıksa da, güvenlik sektörü tarafından kabul görmüş ve yaygın şekilde kullanılmaya başlamıştır. Tabi güvenlik ürünleri üreticileri için de yeni bir pazar oluşturması, bu terime sıkı şekilde sarılmalarında etkili olmuş olabilir.

Aşağıda bir APT saldırısının yaşam döngüsü özet olarak verilmiştir;



Şu ana kadar tespit edilen ve en çok ses getiren APT saldırıları Stuxnet vakası olarak görülmektedir. Stuxnet, Iran nükleer programını durdurmak ya da belli bir süre geciktirmek amacıyla yapılmıştır ve Batılı ülkeler tarafından gerçekleştirildiğine inanılmaktadır.
Bir diğer çok ses getiren APT saldırısı ise güvenlik ürünleri üreticisi RSA'e 2011 senesinde yapılan saldırıdır. Bu saldırı yine bir olta e-posta (phishing) ile başlamış ve 0.gün açıkları kullanılarak sistemlere sızılması ile başarıya ulaşmıştır.

2015 senesi ve sonrasında da APT saldırılarının artarak devam edeceği ön görülüyor. Bu saldırılar Stuxnet olayında olduğu gibi devletler arasında olacağı gibi, ticari alanda da kendini gösterecektir. Bu saldırıların çoğunun Phishing ile başladığı düşünülürse, kullanıcı farkındalığının ne kadar önemli olduğu görülmektedir.

Phishing

Phishing – oltalama… Günümüzde en çok kullanılan saldırı yöntemlerinden biridir. Daha çok sahte e-posta gönderimi yoluyla karşımıza çıkan bu saldırılar genelde kullanıcıların erişim bilgilerini almayı hedeflemektedir. Bununla beraber, gönderilen sahte e-posta, kullanıcıyı başka bir sahte web sitesine (phishing site) yönlendirmekte ve ele geçirilmek istenen bilgilerin bu web sitesindeki formlara girilmesi sağlanmaktadır.

2014 senesi içerisinde de pek çok phishing saldırısı yaşanmıştır. Aslına bakılırsa bu raporun ilk sayfalarında yer alan ve ülkemizde de ciddi hasara neden olan Crypto Locker saldırısı, APT başlığında bahsedilen RSA saldırısı, son günlerde DropBox adına açılan sahte siteler hep Phishing saldırılarının örnekleridir.

Bundan sonraki dönemde de Phishing saldırılarının artarak devam edeceği tahmin edilmektedir. Önceki yıllara bakıldığında, Phishing saldırısına hedef olan sektörler içerisinde Finans Hizmetleri ve Ödeme Sistemlerinin toplamda %60-65 bandında bulunmaktadır. Önümüzdeki dönemde de yine bu sektörlere yönelik saldırıların ağırlıkta olacağı tahmin edilmektedir. Özellikle bankalar adına atılan sahte e-postalar ve açılan web siteleri ile PayPal benzeri ödeme sistemleri adına sahtecilik yapılacağı öngörülmektedir.

Finansal sistemlerin yanında Sosyal Ağlar, Bulut Bilişim Siteleri, Devlet Kurumları, Kritik Altyapılar da Phishing saldırılardan nasibini alacaktır.

Mobil

Gelişen teknoloji ve teknolojinin gittiği yön ile birlikte saldırıların şekli de değişmektedir. Son yıllarda mobil cihaz kullanımının gittikçe yaygınlaşması, saldırıların da bu yöne doğru kaymasına neden oldu. Özellikle mobil cihazlarda zararlı yazılım olmayacağı düşüncesi, cep telefonu ya da tabletlere virus bulaşmayacağı düşüncesi kullanıcıları bu saldırıya daha da açık hale getirmektedir. Bu düşünceyle birlikte, bilgisayarlar için alınan güvenlik önlemleri taşınabilir cihazlar açısından göz ardı edilmektedir.

Son yıllarda, özellikle Android tabanlı cihazlara yönelik saldırıların sayısı gittikçe artmaktadır. Buna karşın iOS tabanlı cihazlara yönelik tehditler Android'le kıyaslandığında halen daha düşük seviyelerde seyretmektedir. Bunun en büyük sebebi ise Android tabanlı cihazlara pek çok kaynaktan uygulama yüklenebilmesi ve bu uygulamaların herhangi bir kontrolden geçmemesinden kaynaklanmaktadır.

Önümüzdeki dönemde mobil cihazlara yönelik tehditlerin daha da artması beklenmektedir. Mobil cihaz kullanımının yaygınlaşması ve hemen her uygulamanın mobil sürümünün çıkması saldırı yüzeyinin genişlemesine neden olmaktadır. Kullanıcıların dikkatsizliği ve uygulamanın indirildiği kaynağın kontrol edilmemesi nedeniyle, zararlı uygulamalar daha çok yayılacaktır. Zararlı uygulamaların hedefinde yine telefonda bulunan iletişim bilgileri, konum bilgileri, önemli dokümanlar olması beklenmektedir. Bununla birlikte, özellikle 2-factor authentication dediğimiz, ikincil kimlik doğrulama yöntemlerinin atlatılması için de mobil cihazlar hedef seçilecektir. Bankacılık uygulaması, e-ticaret uygulaması gibi uygulamalarda cep telefonuna gönderilen tek kullanımlık parola (OTP) ele geçirilmesine yönelik zararlıların yaygınlaşması öngörülmektedir.

DDoS

DDoS – **D**istrubted **D**enial **o**f **S**ervice | Dağıtık Servis Engelleme Saldırısı olarak tanımladığımız bu saldırı yöntemi belki de en az teknik bilgi, beceri gerektiren saldırı yöntemidir. Temel olarak bir hedefe, belli bir zaman diliminde, kapasitesinin çok üzerinde istek gönderilmesi sonucu, hedef sistemin hizmet veremez hale gelmesi amaçlanmaktadır.

Bu saldırı, ilgili sistemin kendi kaynaklarının (işlemci, bellek gibi) tüketilmesinin yanında, daha çok hedef sistemin sahip olduğu band genişliğinin doldurulması yöntemiyle gerçekleştirilmektedir. Günümüzde hem dünyada, hem de ülkemizde internet erişim hızlarının yüksek mertebelere çıkması, az sayıda saldırganla bile yüksek trafik hacmine çıkılmasını sağlamaktadır.

Özellikle 2013 senesi içerisinde Spamhaus'a yapılan ve yaklaşık 300 Gbps'lık bir hacme ulaşılan saldırı tarihin en büyük DDoS saldırılarından birisi olarak tespit edilmiştir. Stophaus isimli bir organizasyon tarafından üstlenilen saldırı nedeniyle Spamhaus üzerinden hizmet alan anti-spam uygulamaları kesintiye uğradı ya da güncellenemedi.

Yukarıda da belirttiğimiz gibi bireysel internet kullanıcılarının dahi yüksek seviyede internet hızına sahip olması, önümüzdeki dönemde gerçekleşecek saldırıların çok daha hacimli mertebelere ulaşacağını göstermektedir. Saldırıların her türlü hedefe yönelebileceğini tahmin etmekle birlikte, özellikle devlet kurumlarına ve finans sistemlerine yöneleceğini tahmin etmek zor değil. 2007 senesinde Rusya ile Estonya arasında yaşanan gerginlik sırasında, arkasında Rusya'nın olduğu siber saldırıcı sonucu Estonya'nın neredeyse tüm kamu sistemlerine ait altyapının çökmesi, önümüzdeki dönemde DDoS'un devletler arası bir siber silah olarak kullanılacağını göstermektedir.

Kritik Altyapılar

Siber saldırıların en önemli hedeflerinden biri de şüphesiz kritik altyapıların yönetildiği sistemlerdir. Saldırıların hedefindeki sistemler daha çok enerji altyapıları, üretim tesisleri gibi yerler olmuştur.

Bu raporun farklı başlıklarında zikredilen Stuxnet olayı en bilinen olaylardan biridir. Stuxnet olayı her ne kadar sadece İran'ın nükleer programının hedeflenmesi şeklinde sunulsa da, aslında SCADA sistemlerinin siber korsanların gündemine girdiğinin bir göstergesidir. Bunu anlamak için öncelikle SCADA'nın ne olduğuna kısaca değinmek gerekir.

SCADA – Supervisory Control And Data Acquisition ifadesinin kısaltmasıdır. SCADA sistemleri aslında bir tür Endüstriyel Kontrol Sistemidir. Geniş ölçekli alt yapılarda, sistemlerin izlenmesi ve yönetilmesini sağlarlar. Havacılık, enerji, sanayi gibi pek çok sektörde kullanılan bu sistemler hayati önem taşımaktadır.

Amerikan İç Güvenlik Bakanlığı'na (Department of Homeland Security) bağlı olarak kurulan Endüstriyel Kontrol Sistemleri – Siber Olaylara Müdahale Ekibi (ICS-CERT) bu sistemlere yönelik tehditleri takip etmekte ve saldırı durumlarında müdahalede bulunmaktadır. Sadece bu tip sistemlere özel bir SOME ekibinin kurulması da bu sistemlere yönelik tehdidin hangi seviyelere ulaştığını göstermektedir.

2015 ve sonrasında da Endüstriyel Kontrol Sistemlerine yönelik saldırıların katlanarak artacağını ve yine diğer siber saldırı araçlarındaki gibi devletler arası ilişkilerde bir cephe olarak kullanılacağı ön görülmektedir.

Sağlık Sektörü

Önümüzdeki dönemde siber saldırılardan nasibini alacağı düşünülen bir diğer sektör Sağlık Sektörü'dür. Var oluş sebebi gereği hem ülkemizde, hem de tüm dünyada insanların bir şekilde dahil olduğu Sağlık Sektörü'ndeki kurumlarda pek çok kıymetli bilgi bulunmaktadır. Vatandaşların adı-soyadı, doğum yeri-tarihi, kan grubu, iletişim bilgileri, adres bilgileri, sağlık sorunları, kimlik numaraları vb pek çok bilgi.

Yukarıda zikrettiğimiz bilgilerin ayrıntısı kurumdan kuruma değişmekle beraber çoğu hastanede ve ilgili ülkenin sosyal güvenlik kurumunda bu bilgiler bulunmaktadır. Ayrıca hastanelerin de bilgi alışverişinde bulunduğu merkezi nüfus kayıt sistemi (ülkemizde MERNİS) çok daha fazla bilgi barındırabilmektedir. Bu açıdan sağlık kurumları, siber korsanların iştahını oldukça kabartan birer hedef durumundadırlar.

Şuana kadar çok fazla duyulmasa da, sağlık sektöründeki güvenlik önlemlerinin yeterince iyi olmadığı bilinmektedir. 2014'ün son günlerinde yaptığımız bir araştırmada, bir devlet hastanesinde bulunan zafiyetler zinciri nedeniyle 600.000'den fazla hastaya ilişkin kritik kimlik bilgileri, iletişim bilgileri ve hastalığın ifşa edilebildiği görülmüştür. Bu zafiyet Sağlık Bakanlığı'nın ilgili birimleriyle paylaşılarak giderilmesi sağlanmıştır.

Tüm bunlar, sağlık kurumlarının sahip olduğu verilerin sızdırılmasına yönelik tehditlerin artacağını göstermektedir. Bu tehdit sadece ülkemizde değil, tüm dünyada etkisini arttırmaktadır.