PHISHING:
İNTERNET DENİZİNİN POPÜLER AVLANMA YÖNTEMİ

Şükrü ALATAŞ
Gazi Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
İktisat Bölümü,
salatas@gazi.edu.tr

Murat ATAN
Gazi Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
Ekonometri Bölümü, Yrd. Doç.Dr.
atan@gazi.edu.tr

ÖZET

Phishing çok yeni bir terim olmasına karşın oldukça çabuk yayılarak tüm internet kullanıcılarını tehdit etmekte olan bir tehlike olarak gösterilebilir. Phishing farklı şekillerde kendisini göstermekte olsa da en bilinen anlamıyla mevcut çalışan bir internet hizmetinin taklit edilerek kullanıcıların kandırılması yoluyla kullanıcıya ait önemli bazı bilgilerin ele geçirilmesi ve kullanıcının maddi zarara uğratılması olarak tanımlanabilir. Bu çalışmada phishing tekniğinin planlamasından sonuç kısmına kadar kademe kademe nasıl çalıştığını ve nasıl çok kısa zamanda önemli bir tehdit haline geldiğini anlatmaya çalışacağız.

ABSTRACT

Even though Phishing is a very new term, it has spread very quickly and has become a threat to all internet users. Even though it is used in many different ways, it can be described as duplicating a valid functioning internet service and obtaining important user information by deceiving those users. In this topic we will study Phishing from initial planning to its results and how it became a threat so quickly.

Anahtar Kelimeler: Phishing, Güvenlik, SPAM, Elektronik Dolandırıcılık

1. GİRİŞ

Hiç şüphesiz internet günümüzde hayatımızın vazgeçilmez bir parçasıdır. Günlük hayatta birçok gereksinim internet sayesinde çok kısa sürede karşılanabilmektedir. Bu anlamda internet her geçen gün hayatın bir vazgeçilmezi olma yolunda emin adımlarla ilerlemektedir.

İnternetin sosyal hayat içerisinde bu kadar hayati yer edinmesinin şüphesiz en önemli sebebi kişilere sağladığı kolaylıklardır. Çok fazla çaba sarf etmeksizin kişilere sağladığı olanaklar interneti her geçen gün biraz daha vazgeçilmez kılmaktadır.

İnternetin sağladığı olanaklardan günümüzde en bilinen ve kullanılanlarından birisi de internet bankacılığıdır. Şu an ülkemizde faaliyette bulunan bütün bankalarla internet üzerinden işlem yapılabilmesi mümkündür.

İnternet şubesi olarak adlandırabileceğimiz bu hizmetlerin büyük bir kısmında, kişinin herhangi bir

banka şubesinden gerçekleştirebileceği işlemleri yapabilmesi mümkündür. Bu durum internet şubelerinin sağladığı zaman avantajı başta olmak üzere tüm imkânları ile kişileri her geçen gün biraz daha fazla internet üzerinden bankacılık hizmeti almaya zorlamaktadır.

Kullanıcılara internet şubelerinin sağladığı zaman kazancının dışında güvenlikte diğer bir önemli faktör olarak nitelendirilebilir. Herhangi bir banka şubesinde yapılacak bankacılık işlemi sırasında taşımak zorunda bulunulan para miktarı oranında güvenliğinizde önem kazanmaktadır. Fakat internet üzerinden paraya hiç el dahi dokunmadan büyük miktarlarda para ile dilenilen işlem gerçekleştirebilmektedir.

O halde bu noktada şu soru sorulmalıdır: internet şubelerini kullanmanın güvenlik açısından doğurduğu risklerden ne derece haberdarız? Bu sorunun cevabı ülkemizde bulunan birçok internet şubesi kullanıcısı için yetersiz derecede haberdarızdır. Öncelikle internet şubesinin teknik anlamda taşıdığı açıkların yanında, üçüncü şahısların oluşturduğu sorunlar son birkaç yıldır her yıl katlanarak ivme kazanan bir hızla büyüyen bir tehdit oluşturmaktadır. Şüphesiz bu tip tehditlerin en başında son birkaç yılın en popüler tehdidi Phishing saldırıları gelmektedir.

2. PHISHING

2.1. TANIM VE TEMEL KAVRAMLAR

Phishing, sosyal mühendislik teknikleri kullanılarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenlik isteyen bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir. Phishing kelimesi ingilizce fishing (balık tutma) kelimesinden türetilmiş bir kelimedir. Bu anlamda kurbanlara phish (fish – balık) denilmektedir [9] ve [13].

Balık tutma esnasında avcı balıkları tutabilmek için farklı çeşitlerde oltalar kullanır. Oltaları balıkların fazlaca bulunduğunu gözlemlediği yerlere tutmak istediği balığın cinsine göre belirli şekillerde yerleştirir ve balıkların oltaya takılmasını bekler.

Phishing dolandırıcılığında da sistem benzer şekilde işlemektedir. Birkaç farklı türü olmasına rağmen sonraki bölümde ayrıntılı olarak anlatılacak genel kabul görmüş sistem şu şekilde işlemektedir. İlk olarak günün popüler ve fazla müşterisi bulunan bankası ya da finans kurumu seçilir. Bu balıkların fazla olduğu gölde avlanmayı seçen avcıya benzetilebilir. Daha sonra seçilen kurumun internet şubesi gözlem altına alınır ve mevcut sistemi tespit edilir. Bu tespit örneğin kurumun kullanıcı kodu sistematiği, şifre düzeneği ve benzeri bazı teknik ayrıntılar ile kurumun müşterilerin profili, demografik ve ekonomik yapısı gözden geçirilerek en uygun tuzak (yem) hazırlanır. Bu noktadan sonra hedef sitenin genel kopyası ya da bir benzeri oluşturulur ve yine sonraki bölümde ayrıntıları anlatılacak sistemlerden birisi kullanılarak bir geçici sunucuda sistem çalışır hale getirilir. Bu anda dolandırıcı hazırlamış olduğu e-postaları elinde hazır bulunan posta listelerine SPAM olarak yollar. Bu postalarda banka/finans kuruluşunun sisteminde güncelleme yapılmakta olduğu ve sistemde eksik bilgilerin tamamlanması isteği belirtilir ve altına dolandırıcının daha önceden hazırladığı sitenin adresi belirli gizleme yöntemleri ile kurban aldatılacak şekilde konulur. Bu postaya inanan kullanıcı kendi elleri ile dolandırıcıya kendi önemli (kişisel) bilgilerini verir. Bundan sonra, dolandırıcıya sadece gelen bilgileri toplayıp bu bilgilerle maddi çıkar sağlamak kalmaktadır [8]. En yalın anlatımıyla bu şekilde işleyen Phishing sistemi son birkaç yılda çok geniş bir kitleyi etkilemekte ve her geçen gün kendisini geliştirip yenilemektedir.

Kısaca Phishing tekniği bir tür sosyal mühendislik tekniği olarak insanların kavramadaki yanılmalarından ve algısal zaaflarından faydalanarak insanlardan çıkar sağlamak olarak tanımlanabilir [16]. Şekil.1'de 24 Temmuz 2006 günü Türkiye Cumhuriyeti Merkez Bankasından gelmiş gibi gösterilerek hazırlanan tuzak e-posta gösterilmektedir [11] ve [12].


TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?sid=d3fd99df91df76dfs

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312)310 3646
©TCMB 2006

(Kaynak: İstanbul Emniyet Müdürlüğü Mali Suçlarla Mücadele Büro Amirliği)

Şekil 1. TCMB Konulu Phishing Denemesi Esnasında Kullanılan E-Posta Örneği

2.2 TARİHÇE

Phishing tekniğinin ilk örneğine 2 Haziran 1996 yılında A.B.D'de faaliyet gösteren AOL (American On-Line) firmasına ait haber grubunda rastlanmıştır [1] ve [10]

Bu tarihten 2003 yılı ortalarına kadar olan dönemde genellikle inandırıcılıktan uzak ve salt yazı bazlı e-posta ve haber grubu iletileri ile yapılmakta olan Phishing dolandırıcılığı, 2003 yılının ikinci yarısından itibaren bir evrim geçirmiş ve çok çeşitli teknikler geliştirerek inandırıcılığını ve dolayısı ile popülerliğini her geçen gün artırmıştır. 2003 yılının ikinci yarısının bu kadar farklılaşmasını, göz aldanması sağlaması için alınan geçici alan adları, salt yazı bazlı iletilerden HTML bazlı ve dinamik içeriğe sahip iletilerin alması gibi bazı temel değişiklikler ortaya koymaktadır [10].

Ülkemizde tekniğin kullanılmaya başlaması 2004 yılı sonlarını bulmaktadır. Ancak yurtdışındaki ilk örneklerinde olduğu gibi ülkemizde de ilk örneklerin inandırıcılıktan uzak, oldukça basit tipte olması bu ilk dolandırıcılara amaçlarına ulaşma imkânı vermemiştir. Zamanla gelişen teknikler ile ülkemizde de oldukça geniş kitleleri etkileyen phishing saldırıları yapılmıştır. Şekil 1'de görülen örnek, 2006 yılı içerisinde en çok ses getiren saldırılardan birisine ait tuzak e-postadır [12] ve [17].

2.3 PHİSHİNG TEKNİĞİNİ BENZER DİĞER TEKNİKLERDEN AYIRAN ÖZELLİKLER

Phishing dolandırıcılığı benzer bazı diğer elektronik dolandırıcılık tekniklerine oldukça fazla benzerlikler içermektedir. Phishing tekniğinin en çok benzerlik

gösterdiği diğer bir teknik 419 Tekniği olarak da bilinen "Nijerya Tekniği"dir [2].

Nijerya tekniği, 1990'lı yıllarda Nijerya da büyük bir kitleyi önemli ölçüde etkilemiş bir başka elektronik dolandırılıcılık türüdür. Teknik olarak Phishing ile benzerlikler gösterse de bazı kilit noktalarda Phishing'den ayrılır. 419 tekniğinde kurbanın zaafının ortaya çıkması için aslında olmayan bir büyük kar ortaya konulur. Sonra bu büyük kar'a ortak olabilmek için kurbandan cüzi bir miktar para talep edilir. Vaat edilen büyük kar'ın karşısında ufak kalan bu bir miktar para alındıktan sonra sistem kendisini yok eder ve dolandırma işlemi bitmiş olur. Oldukça sık rastlanan bir şekli söyle örneklenebilir: Dolandırıcı büyükbabasından kalan 1 milyon dolarlık mirası alabilmek için gerekli olan avukat ve diğer masrafları karşılayamadığı için ufak bir miktar yardım istediği bir e-postayı SPAM yöntemlerini kullanarak bir listeye yollar. Postanın içeriğinde yazan milyon dolarlık paradan ona yardım edenlere pay vereceğini de içerikte belirtir. Bu büyük vaat karşısında kandırılan kurban dolandırıcıya istenilen miktarı verir. Bu esnada dolandırıcı ortadan kaybolur ve dolandırma işlemi sona ermiş olur.

Örnekten de anlaşılabileceği gibi 419 tekniğinde e-posta ile bilgilendirme ve toplumun belirli bazı zaaf ve kavrama zorluklarından faydalanma tıpkı phishing tekniğinde olduğu gibi yürütülmektedir. Ancak iki tekniğin ayrıldığı ana nokta phishing'de kurbanın belirli bir mükâfat vaat edilmeksizin kandırılmasıdır. İşte böyle bir mükâfatın olmamasından ötürü kurban sanki normal bir güncelleme işlemi yapıyormuş gibi bilgilerini vermekte ve hatasız kurulmuş bir düzenek içerisinde kesinlikle dolandırıldığını anlamadan bazen haftalar, bazen aylar boyunca normal hayatına devam etmektedir. Bu sayede dolandırıcıya 419 tekniğinde var olmayan derecede uzun sürelerde işlemi sonlandırma ve izini kaybettirme imkânı sunulmaktadır [2].

Bunun dışında 419 yöntemi birebir ya da daha eski iletişim yolları ile de gerçekleştirilebilirken phishing tekniği mutlaka elektronik bir sistem içerisinde işletilmek zorundadır. Bu anlamda 419 tekniği son birkaç yıldır internet üzerinden Nijerya haricinde de birçok ülkeyi etkileyen bir teknik olmuştur.

3. OLAĞAN BİR PHISHING DOLANDIRICILIĞININ AŞAMALARI

Birkaç farklı türü bulunmasına rağmen genel olarak bütün phishing dolandırıcılıkları aynı aşamaları takip ederek işlerler. Bu aşamalar sırasıyla; Planlama, Hazırlık, Yemleme, Toplama, Dolandırma ve Dolandırma Sonrası İşlemler olarak 6 ana kısma ayrılır [9].

3.1 PLANLAMA

Saldırının ilk aşaması olan planlama, hedef firmanın seçimi, kurban profilinin seçimi ve saldırı tipinin tercihi gibi kilit bazı kararların alındığı kısımdır. Saldırıyı gerçekleştirecek olan dolandırıcı işe ilk olarak popüler ve müşterisi fazla olan bir kurumu seçmek ile başlar. Bu kurumun internet sitesinde bulunan zaafların fazlalığı saldırganın işini kolaylaştırmanın yanında aynı zamanda saldırının başarısı açısında da önemlidir. Ayrıca saldırının konusunu oluşturacak firmanın hesaplarından yapılacak para transferlerinin izlenmemesi ya da firmanın bazı kilit işlemleri kayıt altına almıyor olması saldırganın saldırı esnasında ve sonrasında gizli, isimsiz (anonymous) kalmasında büyük fayda sağlamaktadır. Bu da hedef seçimini bu açıkları barındıran firmalara doğru kaydırır. Günümüzde en çok saldırıya maruz kalan iki firma olan PayPal ve e-Gold'u incelediğimizde bu iki özelliği taşımakta oldukları görülmektedir [9].

Hedef firma seçildikten sonra kurban seçimine geçilir. Bu aşamada hedef olarak seçilen firmanın genel müşteri profili izlenir ve bu profile uygun bir saldırı planlanır. Örnek vermek gerekirse genellikle müşteri profili gençler olan bir firma hedef olarak seçilmişse, yapılacak yemleme esnasında kullanılacak e-posta listesinin gençlerin daha çok bulunduğu sitelerden elde edilmiş bir liste olması saldırının başarı şansını artıracaktır.

Kurban profili'de seçildikten sonra sıra hedef firma ve kurban profili göz önüne alınarak seçilecek olan saldırı türüdür. Saldırı türü seçiminde ana kıstas hedef firmanın sitesindeki bulunan zaaflar ve bu zaafların kullanımıdır. Genel olarak kabul görmüş üç farklı saldırı türü vardır. Bunlar Taklit Saldırılar, Direkt e-posta Saldırılar ve Popup Saldırılar'dır.

3.1.1 TAKLİT SALDIRILAR

Terimden de anlaşılabileceği gibi hedef sitenin birebir aynısını ya da çok benzer bir taklidini yapmak olarak açıklanabilecek bu saldırı türünde hedef sitenin bütün bir kopyası bazı belirli programlar vasıtası ile alınır. Sonra bu kopyada girilen bilgileri toplayıp asıl çalışan sisteme geri döndürecek toplayıcı sistemi oluşturulur. Bu türün ana belirleyici özelliği kullanıcılara kurulan kopya sitenin asıl sitenin bir uzantısı ya da kendisi gibi olduğu hissini vermektir. Bunun için DNS saptırması ya da URL saptırması gibi yöntemler kullanılmasıdır. Yapılan bu kopya sitenin ve gönderilen e-postanın uyumu ve inandırıcılığı saldırının başarısını direkt olarak belirleyen faktörlerdir. Bu tip saldırı günümüzde en yaygın olarak kullanılmakta olan saldırı türüdür.

3.1.2 DİREKT E-POSTA SALDIRILAR

Bu tür saldırıda yine kurbana tuzağa çeken bir e-posta bulunmasına karşın taklit saldırılarda bulunduğu gibi bir tuzak site bulunmaz. Bunun yerine sadece kurbanın girdiği bilgileri toplayacak bir toplayıcı sistemi bulunmaktadır. Bu tip saldırılarda veriler direkt olarak saldırı e-posta içerisinde sorulur. Verilerin girileceği kutucuklar ve gönderim butonu e-posta içerisinde yer alır. Gizli bilgilerini gösterilen kutucuklara giren kurbanın gönder butonuna basması ile birlikte veriler saldırganın toplayıcı sistemine ulaşır. Bu noktada eğer saldırgan verileri gerçekte çalışmakta olan sisteme doğru yönlendirirse kullanıcı gerçekte çalışan sisteme girdiğini sanır ki bu da aldatıldığını anlamasını oldukça güçleştirir. Bu tip saldırı taklit saldırı kadar popüler olmamasının sebebi her geçen gün gelişen e-posta istemcilerinin gönderim işlemlerinde kullanıcıyı uyarması ve gönderim işlemlerine getirdiği kısıtlamalardır [9].

3.1.3 POPUP SALDIRILAR

Bu tip saldırı artık günümüzde geçerliliğini yitirmekte olan bir saldırı türüdür. Bu saldırı türünde hedef sitenin mevcut açıklarından faydalanarak sitenin içeriğine müdahale ederek hedef sayfaya girildiğinde bir Popup penceresinin çıkması ve bu pencere vasıtası ile kullanıcıdan bilgilerin istenmesi şeklinde gerçekleştirilir. Bu tür saldırının popülaritesini kaybetmesinin sebebi, artık hemen hemen her bilgisayarın Popup engelleyici özelliği bulunan internet görüntüleyici kullanmasından ve sitelerde bulunan belirli zaaf ve açıkların yüksek oranda kapatılması ile ilgilidir.

3.2 HAZIRLIK

Saldırının hedef firması, hedef kullanıcı kitlesi ve saldırı tipi seçildikten sonra sıra saldırıda kullanılacak sistemi oluşturmaya gelir. Bu aşamaya hazırlık aşaması denilmektedir. Hazırlık aşaması genel olarak beş ana bölümde incelenmektedir. Bunlar; sitenin kopyalanması, tuzağın oluşturulması, toplayıcı sistemin hazırlanması, yemleme sisteminin hazırlanması ve sistemin sunuculara yerleştirilmesidir [9].

3.2.1 SİTENİN KOPYALANMASI

Hedef olarak seçilen firmanın web sitesi bazı programlar vasıtası ile birebir bilgisayar ortamına aktarıldıktan sonra içerisindeki bazı kısımların gerekli düzenlemeleri yapılır. Bu düzenlemeler esnasında saldırgan mevcut sitenin olabildiğince benzeyen bir kopyaya ulaşmayı amaçlar. Bunun için sitenin içeriğinde bulunana bazı bağlantılar ve resimler kurbanın siteye olan inancının artması için mevcut hedef siteye bağlanır. Bu adım taklit saldırı tipinde geçerli olan bir adımdır. Diğer iki farklı saldırı tipinde bu adıma ihtiyaç duyulmaz.

3.2.2 TUZAĞIN HAZIRLANMASI

Sitenin birebir kopyalanmasının ardından yapılacak olan kopyalanan site içerisinde hedef sitede bulunana benzer bir bilgi girişi kısmının konulmasıdır. Bu konulan tuzak, toplayıcı sistem ile birlikte çalışarak girilen bilgileri toplayacak ve saldırıyı amacına ulaştıracaktır. Bu aşamada saldırgan açısından önemli olan nokta bir önceki aşamada da olduğu gibi saldırganı olabildiğince inandırmaktır. Hazırlanan tuzak taklit bir saldırı yapılacaksa kopyalanan sitenin içerisine, direkt e-posta saldırısı ise gönderilecek e-postanın içine, Popup bir saldırı yapılacaksa hazırlanan Popup kutucuğunun içine yerleştirilir.

3.2.3 TOPLAYICI SİSTEMİN HAZIRLANMASI

Bu aşamada kurulan tuzaktan gelecek verilerin uygun şekillerde tutulmasını sağlayacak sistem oluşturulur. Bu sistem genellikle PHP, ASP ya da benzeri dillerle oluşturulmuş kod betiklerinden oluşturulmaktadır. Saldırganın isteği doğrultusunda betik gelen veriyi bir veritabanında tutabilir, e-posta ile saldırgana iletebilir, anında mesajlaşma yoluyla ICQ ya da benzeri programlarla saldırgana iletebilir. Bu seçim tamamıyla saldırganın istemi ve yeteneği ile ilgili bir durumdur. Bu esnada gözden kaçırılmaması gereken bir nokta saldırganın belirli bazı kodlama yeteneklerine sahip olması gerekliliğidir.

3.2.4 YEMLEME SİSTEMİNİN HAZIRLANMASI

Yemleme işlemi için en baştan itibaren belirttiğimiz gibi e-posta sistemi üzerinden yapılmaktadır. Yemleme esnasında yem olarak atılan e-postaların kopyalanarak oluşturulan sitede olduğu gibi inandırıcılık konusunda üzerinde çalışılmış olması gerekmektedir. Şekil 1. yakından incelenirse çok bariz bazı yazım ve imla hataları göze çarpmaktadır. Bu tip hatalar yemin inandırıcılığını yok edecek ve saldırıyı başarısızlığa uğratacaktır. Bu açıdan yemin dikkatlice hazırlanması ve profesyonelliği saldırının başarısı ile birebir orantılıdır. Yine Şekil 1. incelendiğinde görülebileceği gibi taklit saldırı tipinde olan bu saldırıda URL saptırma işlemi yapılmaya çalışılmıştır. **merkezbanka.org** alan adı üzerinden alınan alt alan adı olarak **http://tcmb.gov.tr.teyit.merkezbanka.org** adresi sayesinde kullanıcılar kandırılmaya çalışılmaktadır. Hâlbuki birçok kullanıcı TCMB'nın resmi internet sitesinin **http://www.tcmb.gov.tr** olduğunu bilir. Bu yüzden de verilen örnek inandırıcılıktan çok uzak bir saldırıya aittir.

Daha başarılı sayılabilecek bazı yemleme örneklerinde URL saptırma işlemi esnasında görülen ile gidilen internet adresleri DHTML gibi bazı sistemler sayesinde farklı olarak gösterilmekte ve bu da kullanıcıları inandırma konusunda daha başarılı sonuçlar vermektedir.

3.2.5 SİSTEMİN SUNUCULARA YERLEŞTİRİLMESİ

Önceki adımlar sıra ile gerçekleştirildikten sonra sıra sistemin sunuculara yerleştirilmesine gelmektedir. Bu aşamada saldırganlar en az iz bırakarak en inandırıcı olabilecek çözümü aramaktadırlar. Phishing tekniğinin ilk ortaya çıktığı yıllarda ücretsiz web alanı sağlayan siteler kullanılmaktaydı ki şüphesiz bu sitelerin inandırıcılık konusunda büyük eksikleri vardı. Zaman içerisinde daha inandırıcı olması açısından daha masraflı olan ücretli web alanları kullanılmaya başlandı. Web alanının yanı sıra zaman içerisinde göz yanılgısı sağlayan alan adlarının kullanımı da yaygınlaştı. Örneğin 2005 yılı içerisinde yapılan bir saldırıda hedef alınan Garanti Bankası için kurbanları şaşırtmak amaçlı **www.bank-garanti.com** adresi kullanılmıştır. Bu tip başarılı örneklerin yanı sıra **merkezbanka.org** gibi Şekil 1. de görülebilecek başarısız örneklerde mevcuttur.

3.3 YEMLEME

Yemleme işlemi belki de saldırının en önemli aşamasıdır demek yanlış olmaz. Yemleme esnasında yapılan hatalar sistemin inandırıcılığını yok eder ki bu da bütün bir saldırının başarısız olmasına neden olur.

Yemleme esnasında genel olarak e-posta kullanılır. SPAM olarak adlandırılan istem dışı gönderilen e-postalara phishing postaları da örnek gösterilebilir. E-posta dışında anında mesajlaşma ile telefon aramaları ve GSM sistemi ile IRC ve Chat odaları yolu ile forumlar ve haber grupları yolu ile kurbanlara ulaşılabilmektedir. Bu durumda yemleme yöntemlerini iki ana kısımda incelenecektir. Bunlar; E-posta yolu ile yemleme ve diğer yöntemler ile yemleme'dir [9].

3.3.1 E-POSTA YOLU İLE YEMLEME

SMTP protokolü ilk olarak 1982 yılında o zaman ki sınırlı kullanım alanı içerisinde oluşturulmuş bir protokoldür. Zaman içerisinde birkaç revizyondan geçmiş olsa da çok ciddi güvenlik zaaflarını bünyesinde bulundurmaktadır. En son Nisan 2001 tarihinde değişikliğe uğrayan SMTP Protokolü RFC2821 referansı ile yayımlanan bu son değişiklik metninin 7. kısım 1. bölümünde açık olarak SMTP protokolünün her türlü saldırıya açık ve güvenlik zaafları bulunan bir protokol olduğu kabul edilmiştir. Sistemi geliştirenler tarafından bile kabul edilen bu zaaflar phishing ve benzeri birçok farklı saldırının e-posta tabanlı olarak geliştirilmesine olanak sağlamaktadır. Bu konuda farklı çalışmalar yapılmaktaysa da henüz toplum tarafından kabul gören bir sonuca ulaşılamamıştır.

Bu noktada sorulması gereken bir soru, nasıl olmaktadır da saldırıyı gerçekleştirecek kişiler yemleme için kullanacakları postaları ele geçirmektedirler? Bu noktada phishing'in atası olarak sayılabilecek SPAM sisteminden yardım almakta ve onun bazı tekniklerini benimsemektedir. Bu tekniklerden en bilineni sayfa taraması yöntemidir. Bu yöntemde saldırgan piyasada bulunana sayfa filtreleme programları yardımıyla arama motorları ya da başka bazı yöntemler sayesinde ulaştığı sayfaları ve bunlara bağlı sayfalardan e-posta adreslerini ayıklamakta ve kendisine bir gönderim listesi oluşturmaktadır. Bu konuda verilebilecek bir istatistik A.B.D. Ulusal Ticaret Komitesi tarafından yapılan bir araştırmaya göre internet sitelerinde verilen her 100 e-posta adresinden 86'sına, haber gruplarında verilen her 100 posta adresinden yine 86'sına SPAM olarak adlandırılan istem dışı postalar gelmektedir. Bu açıdan değerlendirildiğinde internet üzerinde farkında olmadan bırakılan e-posta adresleri büyük oranda saldırganlar tarafından ele geçirilmekte ve bu postalar phishing ve başka saldırılara konu olmaktadır [7].

Değinildiği üzere çeşitli şekillerde toplanan e-posta adreslerinden sonra geriye kalan iş daha önceden hazırlanmış olan postaları listede bulunan adreslere göndermektir. Ancak bu noktada saldırganın izini belli etmemesi için Proxy geçitlerini ve isimsiz (anonymous) posta gönderim araçlarını kullanması gerekmektedir. SMTP protokolünde bulunan açıklardan faydalanan isimsiz posta gönderim araçları, gönderimi yapılan postayı istenilen bir posta adresinden geliyormuş gibi gösterebilmektedir. Şekil 1. deki örnek üzerine devam edersek bu tip bir postanın teyit@tcmb.gov.tr adresinden gelmesi durumunda inandırıcılığının kat ve kat artacağını söylenmesi yanlış olmaz.

Bu noktada saldırgana çıkan engel SPAM postaları engellemesi için geliştirilmiş anti-SPAM (SPAM önleyici) filtre programlarıdır. Bu programlar belirli bazı SPAM tekniklerine göre geliştirilmiş programlardır ve SPAM postaların kullanıcılara ulaşmasını engellemek için oluşturulmuşlardır. Bu noktada anti-anti-SPAM olarak adlandırılan bir düşünce sistematiği ile SPAM olarak filtre tarafından yakalanması mümkün olan posta, filtre programının zaafları araştırılarak SPAM kategorisinden çıkartılmaya çalışılır. Örneğin bu tip filtreler mesajın içeriğinin boyutuna göre aynı boyutta ve çok sayıda yakın zamanlı gönderilmiş postaları SPAM olarak algılamaktadır. Bu engeli aşmak için saldırganlar postaların içine gözükmeyecek bir biçimde gelişi güzel karakterler yazdırmaktadırlar ki bu sayede filtre farklı boyutlarda olduğundan postaları SPAM olarak nitelendirmemektedir. Bu şekilde örneklendirilen filtreleri yanıltma işlemi bir kedi-fare oyununa benzemektedir. Filtrelerin yeni bir gelişim göstermesinin ardından saldırganlar bu gelişimi aşmak için yeni bir teknik geliştirirler. Bu da yine filtrelerin bu yeni geliştirilen tekniği fark edip ona uygun güncellemeleri yapması şeklinde devam eden bir süreçtir.

3.3.2 DİĞER YÖNTEMLER İLE YEMLEME

E-posta yönteminden başka anında mesajlaşma ve forumlar yolu ile olmakla beraber birçok farklı iletişim yöntemi ile yemleme yapılabilmektedir.

Son yıllarda yaygınlaşan internet teknolojisi ile birlikte her evde bulanan internet sayesinde iletişim ve haberleşme anında mesajlaşma (instant messaging) programlarının tekeline geçmeye başlamıştır. Bu tür programlar içerisinde en bilineni olan ICQ'dan başka MSN Messenger, Yahoo Messenger da oldukça yaygın kullanılan programlardır. Bu programlar vasıtası ile yapılan saldırılar son birkaç yılda oldukça yüksek oranlarda artış göstermiştir. Bunun sebebi biraz daha bilinçlenen kullanıcılar ve gelişen filtreler sayesinde inandırıcılıkları azalan phishing saldırılarının kendilerine yeni güvenilir bir iletişim alanı bulma çabalarıdır. Anında mesajlaşma ile yapılan saldırılarda ilk olarak bu tip programları aktif olarak kullanan ve arkadaş sayısı olarak fazla olan bir kurbanın mesajlaşma yazılımında kullandığı şifresi ele geçirilerek, kurbanın listesinde bulunan bütün arkadaşlarına yemleme postası benzeri birer ileti gönderilir. Bu sayede arkadaşından gelen iletiyi dikkatlice incelemeden iletide yazanları yapan kullanıcılar saldırganın istediği bilgileri kendi elleri ile teslim etmiş olmaktadırlar.

3.4 TOPLAMA

Saldırganın hazırladığı tuzağa aldanan kurbanların girdikleri verilerin toplanması işlemine toplama denilmektedir. Toplama işlemi bazı zamanlar bir web sitesi ya da bir veritabanı üzerinden olabileceği gibi bazen de e-posta ya da anında mesajlar olarak ta olabilir. Örneğin saldırganın oluşturduğu sistem her bir kullanıcı bilgisini girip tuzağa düştüğü anda kendisine bilgileri içeren bir e-posta gönderilmesini sağlayabilir. Saldırganın planlarındaki bilgi sayısı ya da belirlediği süre dolduktan sonra sistem kapatılmakta ve toplanan verilerle birlikte diğer aşama olan dolandırma aşamasına geçilmektedir. Burada önemli olan bir bilgi; ortalama olarak phishing saldırısına konu olan sitelerin ömürlerinin en fazla iki gün olmasıdır.

3.5 DOLANDIRMA

Bu aşama elde edilen verilerle birlikte hedeflenen paranın saldırganın eline geçmesi işlemi olarak tanımlanabilir. Şüphesiz ki saldırının en başından beri sürekli olarak kimliğini gizlemeye çalışan saldırganın bu son aşamaya gelirken paraları kendi şahsi hesaplarına aktarması biraz saçma olacaktır. Çünkü bu şekilde yapılacak bir aktarım sonucunda saldırgan izini kolaylıkla belli edebilir. Bu noktada terim olarak "katır" (mule) olarak tanımlanan paravanlar işin içine girmektedir. İlk olarak saldırganlar genellikle Avrupa Birliği ya da A.B.D.'de gazete ya da internet ilanları ile paravanlara ulaşır. Özellikle bu iki yerden aramalarının sebebi hemen hemen bütün finansal kuruluşların bu iki yere para transferi yapabilmeleridir. Verilen ilanda Asya ya da Afrika da bulunan bir firmaya ilanın verildiği yerdeki bulunan para aktarımlarını yapacak çalışanlar arandığı yazılır. Bu tip bir çalışma sonucunda çalışanlara %5 – %10 gibi komisyonlar verileceği söylenir. Bu ilana başvuran kişilerden yerel bankalarda hesap açmaları istenir ve bu hesaplara elde edilen şifreler vasıtası ile dolandırılan hesaplardan para transferleri yapılır. Bu para transferlerini alan paravan, WesternUnion ya da MoneyGram gibi popüler ve yaygın para gönderme yollarından birisi ile saldırganın sahte kimlik ve belgelerle varmış gibi gösterdiği kişilere paranın büyük kısmını gönderir. Bu şekilde para aklanmış olur. Kurbanların işin farkına varması ve olayı gerekli mercilere iletmesi sonucunda ulaşılan bir firmada çalıştığını sanan paravandan başkası olmaz [9].

3.6 DOLANDIRMA SONRASI İŞLEMLER

Tahmin edilebileceği gibi dolandırma işleminin sonunda kullanılan araçlar yok edileceği gibi kullanılan paravanla ilişki de kesilir. Bazı kaynaklarda yapılan büyük çaplı dolandırıcılıklardan sonra ülke ve kimlik değiştirmeye kadar giden işlemlerin yapıldığı belirtilmektedir.

4. KORUNMA VE İSTATİSTİKLER

4.1 PHİSHİNG 'DEN KORUNMA

Phishing saldırısına maruz kalmak günümüzde oldukça olağan bir durumdur. Bazılarımızın farkına bile varmadan SPAM postaları içerisinde kalan saldırı yemlerinden korunmanın bilinen kesin bir yönetimi yoktur. Önceden değinildiği üzere web sayfalarına yazılan e-posta adresleri her daim SPAM ile karşı karşıya kaldıkları göz önüne alınarak banka gibi güvenli yazışmalar için farklı bir e-posta adresi kullanmak bir çözüm olarak düşünülebilir. Bunun yanında ülkemizde defalarca kez bankaların ortak açıklamalarında değinildiği üzere hiçbir şekilde e-posta yoluyla bilgi güncellemesi istenmeyeceği de göz önüne alınmalı ve her bu tür e-posta ile karşılaşıldığında silinmesi ve ilgili kurum konu ile ilgili olarak bilgilendirilmesi phishing'den korunmada bilinen en etkili yöntemdir [15]. Bu kadar basit bir biçimde korunulabilinmesine rağmen phishing nasıl olurda her geçen yıl katlanan hızlarla büyüyen bir tehdit olabilmektedir. Bunun cevabı oldukça basit olarak kullanıcıların bilgilendirilmemesi ve kullanıcıların dikkatsizliği olarak gösterilebilir. Bununla beraber kullanıcıların kullandıkları programları sürekli olarak güncel tutmaları da diğer

bir yardımcı etken olarak sayılabilir. Günümüzde en çok kullanılan üç internet gösterimcisi olan Internet Explorer, FireFox ve Opera'nın son sürümleri ile beraber birer phishing denetleyicisi bulunmaktadır. Bu sayede girdiğiniz bir site eğer phishing amacıyla oluşturulmuş bir sayfa olduğunda görüntüleyiciniz sizi uyarmakta ve sayfanın gösterimini engellemektedir.

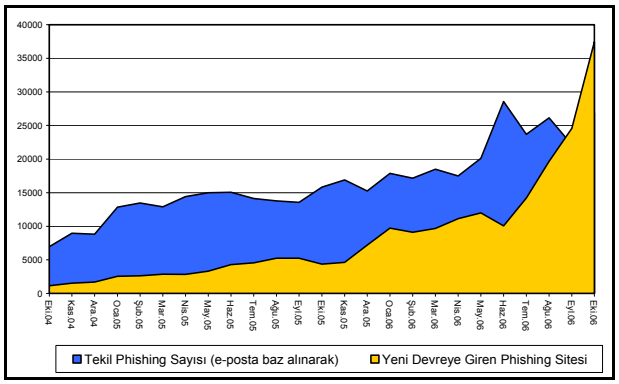
Bu anlamda bilinçli ve dikkatli davranıldığı sürece phishing büyük bir tehdit unsuru olarak görülmemelidir. Bu tip kullanıcı bilinçlendirmesinin yanı sıra firmalarında bilinçlenmesi sayesinde phishing bir tehdit olmaktan çıkacaktır. Firmalar açısından en önemli unsur sürekli olarak müşterilerini e-posta, televizyon, radyo ve basılı medyalar aracılığı ile bilinçlendirme çalışmaları yapmalarıdır. Bunun yanında mevcut kullandıkları sistemlerde saldırganların faydalanabileceği açıkları önceden tespit etmek ve bu açıkları kapatacak güncellemeleri de yapmak büyük önem taşımaktadır.

4.2 SOSYAL OLUŞUMLAR

Anti-Phishing Working Group (APWG) phishing saldırılarını önlemek ve bu konuda bir platform oluşturmak için kurulmuş kar amacı gütmeyen bir organizasyondur. 2600'den fazla üyesi ve 1600'den fazla destekçi firması bulunan organizasyon konuyla ilgili bilgilendirme ve kamuoyu oluşturma amacıyla çalışmalarına devam etmektedir. APWG den başka PhishTank yine kar amacı gütmeyen tamamıyla gönüllülerin oluşturduğu bir topluluktur. PhishTank sitesi, üyelerinin tespit ettiği saldırıları yayınlar ve yine diğer üyelerinin de haberdar olmasını sağlar. Aynı zamanda APWG de olduğu üzere PhishTank'de toplumu bilinçlendirme ve kamuoyu oluşma görevini de üstlenmiştir [4] ve [14]. Bu iki organizasyondan farklı olarak yalnızca Phishing ile mücadeleyi hedef olarak almamış olmasına rağmen MAAWG (Messaging Anti-Abuse Working Group) da bu konuda önemli çalışmalar yapmakta ve halkın bilinçlendirilmesini amaç edinmektedir [4].

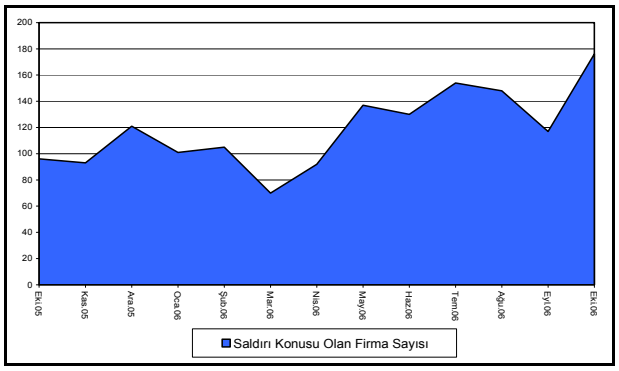
4.3 İSTATİSTİKLER

Konuyla ilgili APWG'nin yapmış olduğu çalışmalar sonucunda her ay sonunda çıkartmış olduğu bültenlerden oluşturulan Şekil 2. ve Şekil 3. den görülebileceği gibi phishing olabildiğince hızlı bir şekilde artış göstermektedir. Şekil 2.'de iki senelik dönem içerisinde tespit edilen phishing sayısının yaklaşık olarak beş kat artış gösterdiği görülebilir. Aynı zamanda yeni devreye giren phishing sitesi sayısının da iki senelik dönem içerisinde yaklaşık 30 kattan fazla arttığını görebilmektedir [3], [5] ve [6].



(Kaynak: Anti-Phishing Working Group Ekim 2005 ve Ekim 2006 Tarihli Bültenleri)

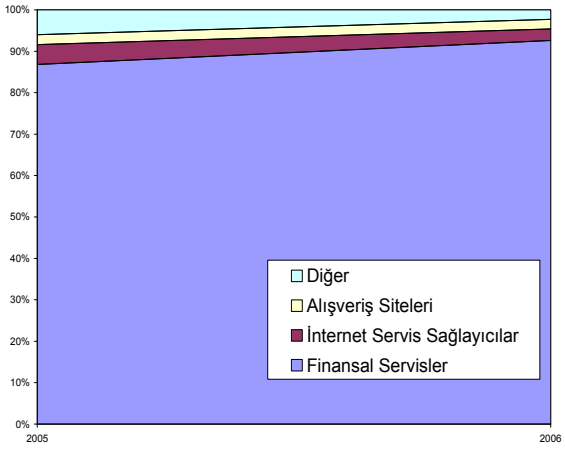
Şekil 2. Ekim 2004 – Ekim 2006 döneminde Tekil Phishing Saldırı Sayısı ile Yeni Devreye Giren Phishing Sitesi Sayısı



(Kaynak: Anti-Phishing Working Group Ekim 2005 ve Ekim 2006 Tarihli Bültenleri)

Şekil 3. Ekim 2005 – Ekim 2006 Dönemleri Arasında Phishing Saldırısına Maruz Kalan Firma Sayısı

Bunun yanında Şekil 3'ü incelediğinde; saldırı konusu olan firma sayısının bir yıllık dönem içerisinde yaklaşık iki kat arttığı görülebilmektedir.



(Kaynak: Anti-Phishing Working Group Ekim 2005 ve Ekim 2006 Tarihli Bültenleri)

Şekil 4. 2005 – 2006 Döneminde Phishing Saldırısına Konu Olan Sektörlerin Yüzde Olarak Gösterimi

Şekil 4 incelendiğinde ise, bir yıllık süre içerisinde phishing saldırılarının hangi sektöre ait siteleri konu aldığına ait veriler görülebilir. Ekim 2005 ve Ekim 2006 dönemlerini kapsayan verilerde görülebildiği gibi saldırıların çok büyük bir kısmı finans sektörünü hedef almaktadır.

5. SONUÇ

Her geçen gün biraz daha hayatımızda yer edinen internet ve internetin beraberinde getirdiği kolaylıkların bir yansıması olarak günden güne çeşitlenen saldırılardan son yıllarda çok hızlı bir şekilde büyüyen ve gelişen phishing saldırısı, korunması oldukça basit olmasına rağmen bilinçsizlik ve dikkatsizlik sonucunda büyüyerek daha büyük kitleleri tehdit eder konuma gelmiştir. Kullanıcıların bu konuda bilinçlendirilmesi ve aktif denetim sayesinde phishing bir tehdit olmaktan çıkacaktır.

KAYNAKÇA

[1] "A Brief History of Phishing", http://www.washington.post.com/wpdyn/articles/A59350-2004Nov18_2.html , Washington Post

[2] "Advance Fee Fraud", http://en.wikipedia.org/wiki/419fraud , Wikipedia

[3] "Anti-Phishing Groups Outline Best Practices", http://www.clickz.com/showPage.html?page=3622972 , ClickZ Internet Marketing Solutions

[4] "Anti-Phishing Working Group", http://www.antiphis hing.org/ , Anti-Phishing Working Group

[5] Anti-Phishing Working Group, "Phishing Activity Trends Report", Ekim 2005

[6] Anti-Phishing Working Group, "Phishing Activity Trends Report", Ekim 2006

[7] "Email Address Harvesting: How Spammers Reap What You Sow", www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm , Federal Trade Commission

[8] "İnternette yeni korsanlık: Phishing", http://www.ntv msnbc.com/news/225998.asp , NTVMSNBC

[9] James L, "Phishing Exposed", Syngress Publishing, Kasım 2004

[10] "Know your Enemy: Phishing", http://www.honeynet. org/papers/phishing/ , The Honeynet Project & Research Alliance

[11] "MB logolu e-posta ile PHISHING (OLTA) Dolandırıcılığı", http://mali.iem.gov.tr/sayfa/detay.asp?id=109 , İstanbul Emniyet Müdürlüğü Mali Suçlarla Mücadele Şube Müdürlüğü

[12] "Merkez Bankası adıyla dolandırıcılık", http://www. ntvmsnbc.com/news/380598.asp , NTVMSNBC

[13] "Phishing", http://en.wikipedia.org/wiki/Phising , Wikipedia

[14] "PhishTank", http://www.phishtank.com/ , PhishTank.

[15] "RSA Security", http://www.rsa.com/go/wpt/ wpindex. asp?WPID=755 , RSA Security

[16] "Social Engineering", http://sozluk.sourtimes.org/show.asp?t=social+engineering , Ekşi Sözlük

[17] "TCMB Teyit İşlemi", http://sozluk.sourtimes.org/show.asp?t=tcmb+teyit+islemi , Ekşi Sözlük