Phishing Rehberi

Özet

Phishing, günümüzde yaygın olarak kullanılan bir saldırı yöntemidir. Görsel ve yazılı basında son zamanlarda online dolandırıcılık adı altında sık sık haberler duymaktayız. Phishing yönteminde temel kullanıcıyı kandırarak, kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaralarından bu hesaba ait internet şifresine kadar birçok özel bilgileri ele geçirmektir.

Kullanılan yöntemlerin başında e-posta ile gönderilen sahte mesajlar gelmektedir. Bu e-posta sanki bir ticari kurumdan(bankalar, alışveriş siteleri vb.) geliyormuş gibi bir izlenim yaratır. Bu, kullanıcının kendisine ilişkin bilgilerini girmesi için kuruma ait bağlantıya(link) tıklamasını içeren bir e-posta olabilir. E-posta içeriği kişisel bilgilerin güncellenmesi, sistemdeki yeniliklerin hesabınızda aktif olması için şifrenizi girin gibi mesajlardır. Bunu gören kullanıcı e-posta ile gelen mesajdaki bağlantıya tıkladığında kurumun web sitesinin birebir kopyası olan başka bir sayfaya yönlendirilir. Burada girilen şifre gibi özel bilgiler artık başkasının eline geçer.

1. E-Posta Trafiği

İnternet dünyasının en çok kullanılan birimlerinin başında e-posta kullanımı gelmektedir.
Artık bir çok insan gündelik işlerini e-posta ile takip eder hale geldi. İnternetten alışveriş yapıldığında, yapılan bu alışverişe ait fatura bilgileri e-posta vasıtasıyla da gönderilmekte, online bankacılık işlemleri, bankada sıra beklemeden internet üzerinden gerçekleştirilebilmekte ve yapılan bu işleme ait bilgilerde e-posta ile müşteriye bilgisi dahilinde ulaşır. E-posta kullanımının günden güne artması beraberinde bazı sorumluluklarda getirmiştir. İnternet kullanıcıları artık e-posta hesaplarında beklenmedik sürprizlerle karşılaşıyor. İstenmeyen e-postalardan(Spam), virüslere kadar bir çok eylemler e-posta yoluyla gerçekleşmeye başladı. E-postanın günlük hayatta vazgeçilmez bir parça haline gelmesi bazı kesimlerin iştahını kabarttı. Online dolandırıcılık buna paralel olarak arttı. E-Posta kullanımındaki artış vesilesiyle, kötü niyetli biri, bir kuruma ilişkin özel bilgileri(kullanıcı adı, bu kullanıcının şifre, kredi kartı numarası vb.) ele geçirmek için e-postayı kullanır. Bu şekilde e-posta ile yapılan dolandırıcılığa ***phishing*** adı verilmektedir.

Phishing yöntemi özellikle yurtdışında başvurulan bir yöntemdir. Son zamanlarda phishing saldırılarında temel hedef Citibank, eBay ve PayPal müşterileri oldu. Ülkemizde bu yöntemle yapılan saldırılara pek karşılaşılmasa(nadiren) da kullanıcıların bilinçlenmesi sonucunda olası bir tehlikeye karşın önceden tedbir almalarında fayda vardır. Yurt dışında bu konuda yapılan anket sonuçları phishing yönteminin önemi vurgulandı. Bu yöntem ile ele geçen şifrelerle kullanıcıların banka hesaplarına girildiği ve internet kullanıcılarını büyük zarara soktuğuna dikkat çekiliyor.
Uzmanlar, dolandırıcıların ele geçirdikleri hesap numaraları ve şifrelerle, internet üzerinden kullanıcının banka hesabına bağlanarak para çaldıklarını açıkladı.

2. Phishing Tehlikesi

Phishing atakları, kullanıcıları şüpheye düşürmemek ve onların güvenini kazanmak için çeşitli yollara başvurur. Internet kullanıcısının aklını çelip, phishing olayının gerçekleşmesi için tek gereken kullanıcının e-posta mesajındaki bağlantıya tıklayıp karşısına çıkan sayfadaki girdileri(kredi kartı, finans bilgileri, şifre vb.) doldurması yeterli olur. Ekrana çıkan sayfa kurumun bire bir benzerinden oluşan bir sayfadır. E-Posta ile gelen mesaj içeriğine örnek olarak;

"Sayın müşterimiz,

Bankamızın bilgisayar sistemini yenileme ve bu sisteme ait alt yapımızdaki değişiklikler nedeniyle online olarak işlem yapabilmeniz için hesap bilgilerinizi güncellemeniz gerekmektedir. Hesap güncelleme işlemini yapabilmeniz için aşağıdaki bağlantıyı kullanarak yapabilirsiniz.

http://bankamiz.www.web/?jklemdsewk4254gtrxcb54747rw

Saygılarımızla,

Bankamız.www Bilgi İşlem Müdürlüğü"

Yukarıdaki bağlantı, müşterinin İnternet bankacılığını gerçekleştirdiği kuruluşun web içeriği olarak aynısıdır. Müşteri bu işlemden kuşkulanmaz ve bağlantıya tıklarsa karşısına hesap numarası ve şifresini soran pencere gelir.
Bu pencerede istenilen bilgileri girdiğinde müşteriye ait özel bilgiler artık başkasının eline geçmiştir.

Dear Sovereign customer,

We recently reviewed your account, and suspect that your Sovereign Internet Banking account may have been accessed by an unauthorized third party. Protecting the security of your account and of the Sovereign network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your Sovereign Internet Banking account. In case you are not enrolled for Internet Banking, you will have to use your Social Security Number as both your Personal ID and Password and fill in all the required information, including your name and your account number.

2. Review your recent account history for any unauthorized withdrawals or deposits, and check your account profile to make sure not changes have been made. If any unauthorized activity has taken place on your account, report this to Sovereign staff immediately.

To get started, please click the link below:

https://www.site-secure.com/cgi-bin/cgig2.exe/sovbank/SID/GetLogon

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Sovereign system. Thank you for your prompt attention to this matter.

Sincerely,

The Sovereign Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your Sovereign account and choose the "Help" link in the header of any page.

***** Yabancı kaynaklı bir e-posta. Bu e-posta kurumdan gelmiş gibi müşteriye gönderilmiştir.

***** Bir bankaya ait tuzak web sayfası. Açılan penceredeki bilgileri dolduran kullanıcı, özel bilgilerinin başka şahısların eline geçeceğinden habersizdir.

Son zamanlarda eBay, Yahoo, MSN, Paypal, Citibank, Earthlink kullanıcılarına yönelik phishing saldırılarında gözle görülür oranda artış olduğu belirtiliyor. Kullanıcıların şifrelerine ve finansal bilgilerini ele geçirmek için e-posta yoluyla gönderilen maillerin içeriğine dikkat edilmesi gerekir.

Müşterisi olduğu kuruluştan hediye paketi kazandığını belirten bir e-posta alan İnternet kullanıcısının tüm dikkatinin bu elektronik postada olacağı aşikârdır. Hediye paketinin adresine gönderilmesi için e-postada belirtilen bağlantıyı ziyaret edip gerekli bölümleri doldurulması istenir. Bunların başında da sayfadaki form alanına müşteri numarasının ve şifresinin yazılması istenir. Sonrasında bu veriler akıp gider.

3. Phishing örnekleri

Aşağıda kullanıcıyı kandırmak için gönderen olarak kullanılan e-posta adresleri(genellikle sahte adreslerdir), e-posta içerikleri, hedef alının kullanıcılara ilişkin bilgilere dair örnekler bulacaksınız. Örnekler son zamanlarda artan phishing ataklarına karşın kullanıcıları bilgilendirmek için verilmiştir. Bu bölümdeki phishing örnekleri Anti-Phishing Working Group (APWG) internet adresinden alınmıştır.

**** Gönderici olarak görülen e-posta adresi :*** MSNPay@MSN.com
E-Posta başlığı **:** Your membership will be cancelled
Hedef kitle **:** MSN kullanıcılar
Ele geçirilmek istenen bilgiler: Kredi kart bilgisi, kişisel bilgiler.

Kullanıcıya gönderilen e-postadan kesit:
"Darling MSN services client,

During one of regular automated verification procedures we've encountered

a trouble caused by the fact that we could not verify the data that you provided to us.

Please, give us the following information so that we could full verify your identity.

Otherwise your access to MSN services will be deactivated.

To verify your data please follow this link https://start.msnupdateting.info/track?billing

Thank you for using MSN.

MSNPayments Center."

E-postada belirtilen bağlantı ziyaret edildiğinde sahte MSN sitesine kullanıcı yönlendirilir. Fakat site MSN sitesiyle birebirdir. Yani tamamen MSN sitesinin kopyası oluşturulmuştur.

Kullanıcıyı aldatan bu site, kullanıcının e-posta adresini, e-postaya ilişkin şifreyi, kredi kart numarasını ve kişisel bilgilerin ele geçirilmesini sağlar.

**** Gönderici olarak görülen e-posta adresi*** **:** aw-confirm@ebay.com
E-Posta başlığı **:** TKO NOTICE: Verify Your Identity
Hedef kitle **:** eBay müşterileri
Ele geçirilmek istenen bilgiler: Kredi kart bilgisi, kişisel bilgiler.

Kullanıcıya gönderilen e-postadan kesit:
"
Dear eBay customer,

During our regulary scheduled account maintenance and verifications procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons.

1. A recent change in your personal information (i.e. change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below.

https://scgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo

If your account information is not updated within 48 hours the your ability to sell or bid on eBay will become restricted.

"

Yukarıdaki e-posta, kuruma ilişkin logosuyla birlikte kullanıcıya gönderiliyor. Kullanıcı e-posta belirtilen bağlantıya gittiğinde aşağıdaki resimde görüldüğü gibi adresin benzeri olan başka bir sayfaya yönlendiriliyor.

Aslında e-mail içeriğindeki bağlantı adresi gerçekmiş gibi gözükse de daha önceden hazırlanan kurumun sahte internet sayfası gerçeğiyle görünüş olarak aynısı durumundadır.

Kullanıcı buradan kullanıcı kodu, şifre, kredi kartı gibi bilgilerini girdiğinde bilgiler kötü niyetli kişilerin eline geçiyor.

Kullanıcı yönlendirildiği adrese dikkat ederse gerçek eBay adresi olmadığı görülür. Fakat ilk görünüşte olağan dışı bir durum sezinlenmez. eBay sitesiyle birebir aynısı olan bu sahte site görünüş olarak kullanıcıda şüphe uyandırmaz.

**** Gönderici olarak görülen e-posta adresi*** **:** services@paypal.com
E-Posta başlığı **:** Please, update your Paypal account
Hedef kitle **:** Paypal kullanıcıları
Ele geçirilmek istenen bilgiler: Kullanıcıların Paypal bilgileri(Kullanıcı adı ve şifresi)

Kullanıcıya gönderilen e-postadan kesit:

PayPal®

Dear PayPal Customer

This e-mail is the notification of recent innovations taken by PayPal to detect inactive customers and non-functioning mailboxes.

The inactive customers are subject to restriction and removal in the next 3 months.

Please confirm your email address and credit card information by clicking the link below:

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

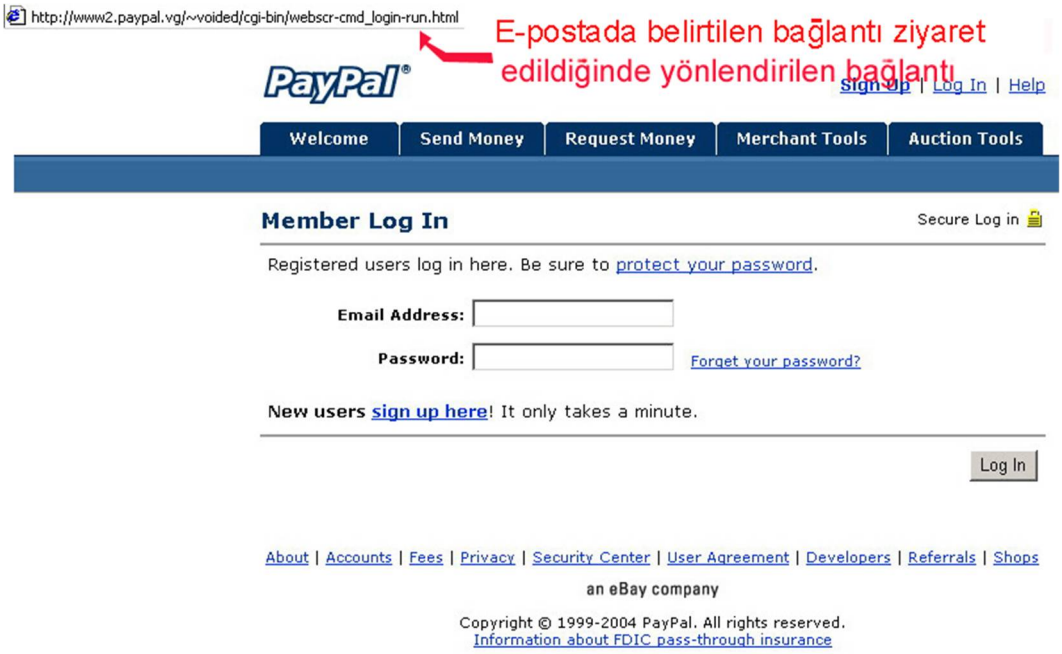
This notification expires April 20, 2004

Thanks for using PayPal!

This PayPal notification was sent to your mailbox. Your PayPal account is set up to receive the PayPal Periodical newsletter and product updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes to your preferences may take several days to be reflected in our mailings. Replies to this email will not be processed.

Copyright© 2002 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

Paypal üyesi bir internet kullanıcısı bu tür bir e-posta ile karşılaştığında bu e-postadaki yönergeyi gerçekleştirmeme olasılığını düşünmek gerekir. Mesajda belirtilen bağlantıya gidildiğinde aşağıdaki sayfaya da belirtilen adrese yönlendirilir. Adrese dikkat edildiğinde bu adresin gerçek paypal adresi olmadığı görülmektedir.



4. Phishing Teknikleri

Kullanıcılar nasıl aldatılmaktadır? Araştırmalarda online dolandırıcılık oranı neden bu kadar artıyor? Phishing ataklarının büyük kısmı ABD'de gerçekleşmektedir. Ülkemizde phishing konusunda yapılan bir araştırma bildiğim kadarıyla mevcut değildir.

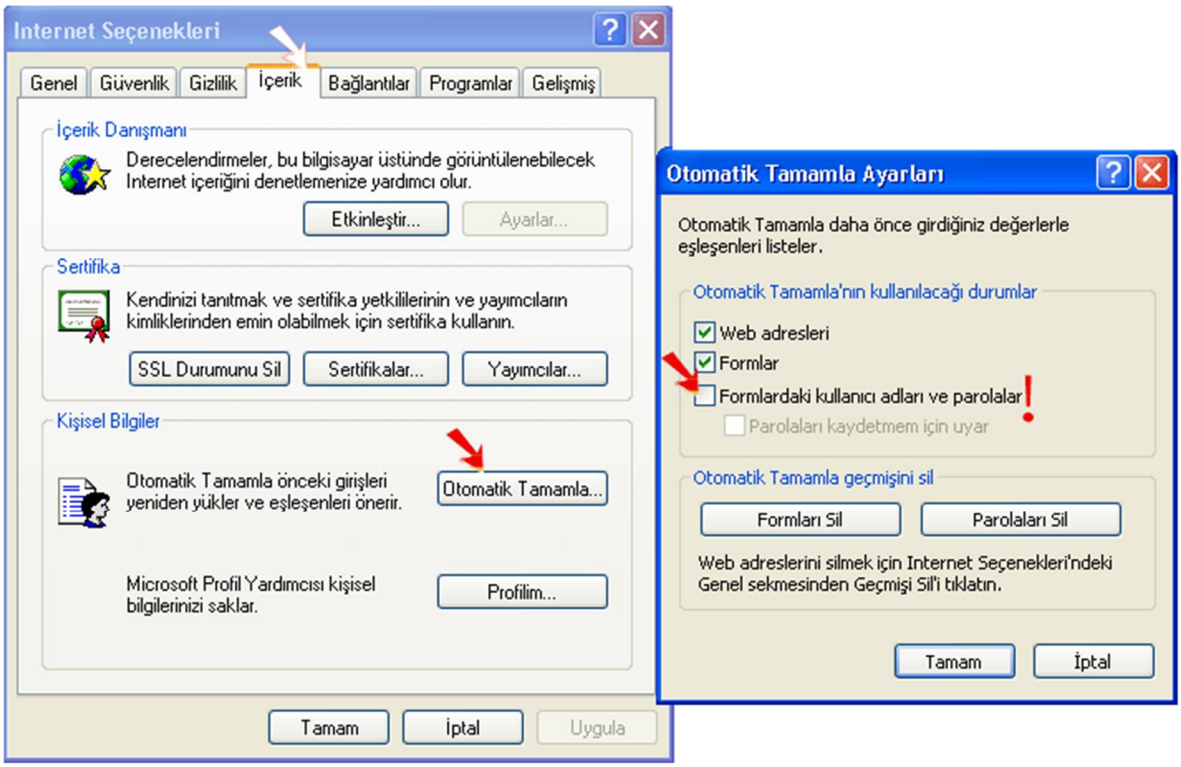
Fakat ülkemizdeki bir bankadan e-posta yoluyla bilgi güncellemesi yapılması gerektiğini içeren bir mesaja rastladığımı da belirtmek isterim. Bu tamamen aldatmaya yönelik bir e-posta idi. Bankalar müşterilerinden e-posta yoluyla bilgi güncellemesi istemezler ya da banka çalışanının müşterisinden internet yoluyla kişisel bilgileri isteme ayrıcalığı yoktur.

Ülkemizdeki banka müşterilerinin online işlem şifrelerinin çalınması büyük oranda keylogger(klavye tuş girdilerini kayıt eden araçlar) vasıtasıyla gerçekleşmektedir. Kullanıcıların sistemine yerleştirilen keylogger, sistemde yapılan tüm işlemlerin bir kaydını tutar. Bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya sistemde bir text dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana gönderilir. Günümüz internet solucanlarının bazıları sisteme entegre olduğunda eğer internet solucanının keylogger özelliği varsa sistemde olup biten tüm kayıtları programcısına gönderir veya ftp(file transfer protocol) aracılığıyla kayıt bilgilerini bir sunucuya aktarır.

Peki keylogger türü programlar sisteme nasıl aktarılıyor?

Bir ya da birden fazla sistemde, sistem güvenirlilik testleri gerçekleştiren uygulamalar mevcuttur. Bu uygulamaların en çok kullanılanlarının başında da port tarayıcılar(portscanner) gelmektedir. Bu port tarayıcı programlarıyla sistemin IP numarasını ya da belirli aralıklardaki IPleri tarayarak açık portlar(dinlemede olanlar) tespit edilir. Saldırgan/saldırganlar port taraması yaptıkları sistemlerde özellikle dosya paylaşımının olup olmadığını kontrol ederler. Eğer paylaşıma açık bir bilgisayar tespit ettiklerinde keylogger uygulamasını sisteme aktarırlar(Paylaşımı olan bilgisayar dışarıdan sisteme girilmeye çalışıldığında şifre sorabilir. Bu şifreyi aşarsa istediğini elde eder). Bu işlemi otomatik olarak yapan programlarda mevcuttur. Herhangi bir uygulama içine eklenen ya da kullanıcıya istediği programmış gibi takdim edilen trojan türü tehlikeli programlarda kullanıcının sistemini uzaktan kontrol edilmesine neden olur. Bu şekilde de kullanıcı izlenip internette gezdiği yerler takip edilir.
Ayrıca son aylarda (haftalarda/günlerde) Windows tabanlı işletim sistemlerinde tespit edilen açıklarla sisteme rahatlıkla uzaktan müdahale edilebilmektedir. Bu müdahalelerin başında sisteme dosya aktarma, aktarılan dosyayı çalıştırma gibi işlemlerle sonrasında kullanıcılar takip edilebilmektedir(bu tür açıklar, yamalarla kapanmıştır). Fakat sistemlerini güncellemeyen kullanıcılar halen tehlike altındadır.

Mecbur kalmadıkça(ve hatta asla) bankacılıkla ile ilgili işlemleri güvenmediğiniz bilgisayarlarda yapmayın. Kullandığınız bilgisayarın web browserin "otomatik tamamlama “özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmın işaretsiz olmasına dikkat edin.



Unique Phishing Attacks by Targeted Company

Phish Target	Jun-04	Jun-04	May-04	Apr-04	Mar-04	Feb-04	Jan-04
Citibank	682	492	370	475	98	58	34
U.S. Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
LLoyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9
Wells Fargo	12	1	0	0	12	0	0
Westpac	11	11	12	17	10	0	3
Halifax	10	11	9	6	1	0	1
MBNA	9	4	1	2	0	2	0
Postbank	9	0	0	0	0	0	0
VISA	9	9	21	0	7	8	2
Nationwide inter	8	2	10	0	0	0	0
HSBC	6	5	3	3	4	0	1
Verizon	6	4	2	0	0	0	0
Woolwich	6	3	3	0	0	0	0

* Phishing ataklarına hedef olan kuruluşlar

Yapılan araştırmalarda en çok phishing ataklarına maruz kalan firmaların başında finansal şirketler, ataklara maruz kalan finansal şirketlerden sonraki sırayı online olarak alışveriş işlemini gerçekleştiren firmalar almaktadır.

Phishing ataklarının en çok gerçekleştiği ülkeler sırasıyla;

1. ABD
2. Güney Kore
3. Çin
4. Rusya

5. İngiltere
6. Meksika
7. Tayvan

Kullanıcıları bu denli zor durumda bırakan phishing ataklarının gerçekleşmesinde temel etmen sistemlerdeki açıklar ve kullanıcıların yeteri kadar bilinçlenmemesidir.

Phishing atak tekniğinin en önemlisi URL (Universal Resource Locator) gizleme tekniği gelmektedir. URL kelimesinden kastımız;
www.yahoo.com / www.hotmail.com / www.ankara.edu.tr gibi internet adresleridir. Bu adreslere karşılık gelen IPler bazı metodoloji işlemiyle değişik şekil alabilir(bu işlemler sonucu ortaya çıkan özel karakterlerin her browserda çalışacağı garantisi yoktur).

Örneğin;

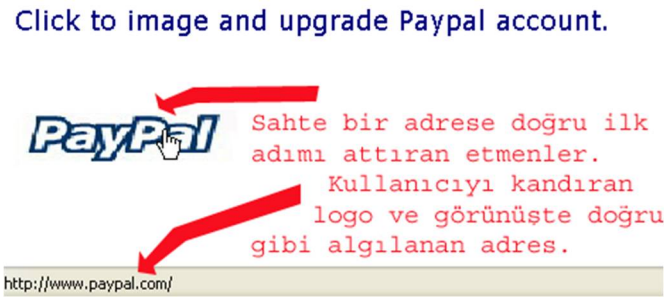
http://bankam.www:finansal@dolandiricilik.www/phishing/sayfa.htm

Bu URLyi web browsera yazıldığında bankam.www internet adresine bağlanılmaz, dolandiricilik.www isimli adrese bağlanılır.

Bir diğer örnek ise IP, Hex normuna dönüştürülür. Bu şekilde IP kullanıcı gözünden saklanır.

http://0xD4.0x9C.0x04.0x14 veya http://0xD49C0414

Atakların gerçekleşmesi için kullanılan açıkların başında İnternet Explorer – Outlook Express gibi internet browserların ve e-posta uygulamalarında bulunan açıklar gelir. Bu açıklar sayesinde kullanıcı e-posta içerisindeki bağlantının üyesi olduğu web sitesine yönlendiriliyormuş hissi vermesine neden olur. Aşağıdaki resimde paypal logosuna tıklamadan önce internet browserin bağlantı sekmesine bakıldığında paypal sitesinin adresi görünmektedir. Gerçekte logo tıklandıktan sonra kullanıcı başka bir adrese yönlendiriliyor.



Yukarıdaki resimde bu tür algılamayı sağlayan kod parçası şu şekle benzer:

```
<A …="http://www.paypal.com/"><M*P name=FPMap0>
<A**A shape=RECT coords=0,6,151,32 href="http://SAHTE.WWW/">
</M*P><I*G height=38 src="paypal.gif" width=156 useMap=#FPMap0 border=0>
</A>
```

Sayfadaki resme tıklandığında SAHTE.WWW adresine kullanıcıyı yönlendirir. Kullanıcıyı yanıltmak için kurumun logo kullanmasının yanı sıra doğrudan bağlantı verip kullanıcıyı sahte bağlantıya yönlendirebilir.

5. Phishing saldırılarından korunma

Unutulmamalıdır ki, phishing saldırıların temelinde e-posta ile kullanıcıları kandırma yatar. Bu tür online dolandırıcılıktan korunmanın en önemli yöntemi bilinçlenmektir.

- E-postanıza müşterisi olduğunuz kurumdan gelen şifre isteklerine kulak asmayın. Bu tür istekler genelde kurum adından gönderiliyormuş gibi yapılır.
- E-postanıza gelen mesajların doğruluğunu ispatlayın. Tanımadığınız kimselerden gelen mesajları silin, asla cevap vermeyin. "Aşağıdaki bağlantıya tıklayın" gibi e-posta isteklerine yanıt vermeyi düşünmeyin.
- Bankalar sizden e-posta ile kişisel bilgi / şifre talebinde bulunmaz. Eğer böyle bir istek gelirse derhal bankanızla irtibata geçin durumu aktarın.
- Online olarak alışveriş yada banka işlemleri yapmak istiyorsanız, bağlandığınız adresin güvenli olup olmadığını kontrol edin(kişisel bilgi/şifre girişi esnasında web browserınızın sağ alt köşesinde kilit simgesi varsa bilgileriniz şifrelenmiş olarak aktarıldığını anlarsınız) .
- Eğer e-postanıza kişisel bilgilerinizi doldurmanızı isteyen bir form sayfası gelirse bu formu doldurmadan 3 kere düşünün. 1. düşünmeniz gereken; gerçekte bu form nereden geldi?. 2. düşünmeniz gereken; bu formu doldurmam neden isteniyor?. 3. düşünmeniz gereken; formu doldurursam neler olabilir?
- Çeşitli kurumlardaki hesaplarınız için kendinizi farklı şifre kullanma konusunda zorlayın.
- Bankanızdan gelen kart extrelerini, hesabınızı düzenli olarak kontrol etmeyi unutmayın. Olası aksiliklerde bankanızla ile irtibata geçin.
- Sisteminizi düzenli olarak kontrol edin. İşletim sisteminizin güvenlik yamalarını yükleyin, Antivirüs yazılımınızı devamlı olarak güncelleyin. Web browserınızın güncel kalmasını sağlayın.
- Güvenmediğiniz bilgisayarlardan banka işlemlerinizi gerçekleştirmeyin.

Tacettin KARADENİZ
tacettin[at]olympos.org

Referanslar

- http://www.antiphishing.org [Anti-Phishing Working Group]

- http://www.olympos.org/article/articleview/252/1/10/ [URL gizleme teknikleri]

- http://www.nextgenss.com [Phishing Study]