

**Caner KOCAMAZ**

**Adli Bilişim Uzmanı**

## **Kimlik Hırsızlığına Karşı Web Tarayıcıların Kullanımı**

### **Kimlik Hırsızlığı Nedir?**

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir. Kredi kartı ve internet bankacılığı bilgileri, şifre ve parolalarınız, elektronik posta, MSN sohbet programı parolalarınız ve diğer önemli kişisel bilgilerinizin bir başkası tarafından çıkar sağlamak amacıyla kullanıldığı bir dolandırıcılık türüdür. Bu makalede internet üzerinden yapılan kimlik hırsızlığına karşı web tarayıcıların güvenlik özelliklerini ele alacağız.

### **Kimlik Hırsızlığının Zararları?**

Her gün onlarca internet sitesine giriyor, onlarca elektronik posta okuyoruz. Kredi kartı ile internet üzerinde alışveriş yapıyor ve bu alışverişlerin dökümünü elektronik posta adresimizden okuyoruz. İnternet bankacılığını kullanarak havale ve EFT işlemleri yapıyoruz. Telefon görüşmelerimizin fatura bilgileri ve yine döküm bilgilerini internetten takip ediyoruz. Sohbet programlarında arkadaşlarımızla sohbet ediyoruz. Kişisel bilgilerin yanı sıra kurumsal bilgilerimizi de internet ortamında aktif olarak kullanıyoruz. Ticari yazışmalarımızın çoğunu yine internet üzerinden gerçekleştiriyoruz.

İnternetin sağladığı bütün bu faydalı işlemler hayatımızı oldukça kolaylaştırıyor. Peki bu kolaylıklar hayatımızı karartan bir kâbusa dönüşebilir mi? Eğer anlattığımız işlemleri yaparken kullandığımız kişisel bilgilerimizi üçüncü şahısların eline geçer ve art niyetli olarak kullanılırlarsa “evet”.

Dolandırıcılar kişisel bilgilerinizi ele geçirerek;

1- Size ait kredi kartı ile alışveriş yapabilir. Banka bilgilerinizi kullanarak EFT, Havale işlemleri yapabilir. Bu işlemleri sizin hesabınızdaki bakiyeyi kullanarak yaptıkları gibi, hesabınızı para aktarma işlemleri için de kullanabilirler.

2- Nüfus bilgileriniz, annenizin kızkılık soyadı gibi bilgilere erişerek sizin adınıza yeni banka hesapları açabilirler hatta şirket bile kurabilirler.

3- Facebook ve MSN Sohbet programında kullanıcı adı ve parolalarını ele geçiren şahıslar sizin adınıza arkadaşlarınızdan para, cep telefonu kontörü talep edebilir.

4- İnternette kullandığınız diğer kullanıcı adı ve parola bilgilerinizi ele geçirerek özel hayatınızı ilgilendiren diğer bilgilere erişebilir hatta bununla size şantaj bile yapabilir.

5- Elektronik postalarınızı takip edebilir, ticari yazışmalarını manipüle ederek çıkar sağlayabilir.

Bugün sadece “Sanal Banka Mağdurları Derneği”ne ulaşan verilere göre dolandırılan ve hesapları boşaltılan binlerce internet bankacılığı mağduru Tablo-1’ de bu durumun vahim bir göstergesi olarak önümüzde duruyor.

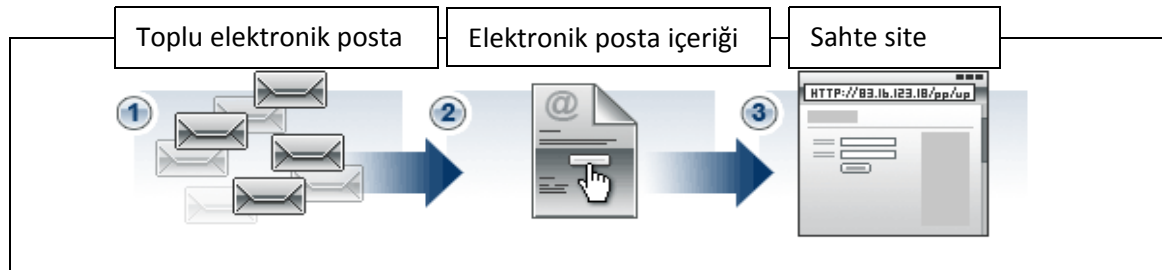
Banka	Mağdur Sayısı	Parası Ödenen Mağdur Sayısı
Garanti Bankası	931	1
İş Bankası	17	
Koçbank	12	
Akbank	49	
TEB	7	3
Yapı Kredi	561	1
Oyakbank	13	
Şekerbank	3	
Vakıfbank	17	
Kuveyt Türk	2	1
Finansbank	4	1
Ziraat	5	
HSBC,Denizbank, Fortis Bank, Tekfenbank, Turkishbank, BankAsya	1	

Tablo 1-Sanal Bankacılık Mağdurları

### Kimlik Hırsızlığı Yöntemleri

Dolandırıcıların günümüzde en sık kullandığı yöntemler Yemleme(Phishing-fişing diye okunur) ve casus programlardır (keylogger,spyware). Bu yöntemlerin yanında sistemlere yetkisiz erişme, sosyal mühendislik, ATM dolandırıcılığı gibi yöntemler de kullanılır.

**a. Phishing:** Bu yöntemde dolandırıcılar banka, kredi kartı bilgilerinizi güncellemeniz için size sahte elektronik posta göndererek (fake mail) kendi yaptıkları sahte siteye (spooft site) girmenizi isterler. Size gelen elektronik postanın gerçek kuruluştan geldiğini göstermek için kuruluşa ait logo ve diğer bilgileri kullanırlar.

Şekil 1(<https://www.paypal.com/./UnderstandPhishing-outside>)

Phishing yöntemi Şekil-1' de kısaca özetlenmiştir. Buna göre;

1- Dolandırıcı bir bankadan geliyormuş gibi görünen mesajı postayı binlerce farklı elektronik posta adresine toplu olarak gönderir. Mesaj içerisinde bir linke tıklanması veya bir telefon numarasının aranması için kurbanı harekete geçirecek, heyecanlandırarak içerikte bilgiler koyar.

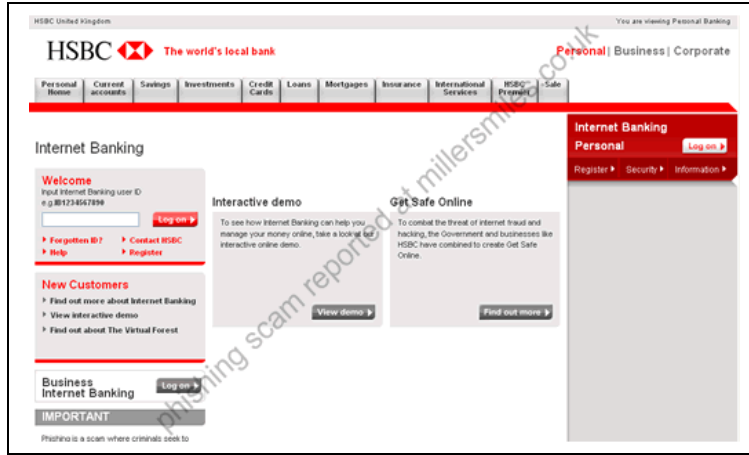
2- Elektronik posta içerisinde sahte siteye yönlendiren bir link veya bir buton vardır.

3- Sahte sitenin görünümü gerçek sitenin bir kopyası olarak hazırlanmıştır. Siteye giriş yapıldığında kişisel bilgiler, kredi kart bilgileri ve parolalar sorulur.



Şekil 2 (www.millersmile.co.uk)

HSBC Bank'tan geliyormuş gibi görünen bu elektronik posta adresinde kullanıcı hesabınızın kısıtlandığını ve sorunu çözmek için linke tıklamanız isteniyor. Linke tıkladığınızda karşınıza gelen ekran ise dolandırıcı tarafından hazırlanmış HSBC Bank'ın sahtesi web sitesi oluyor.



Şekil 3(www.millersmile.co.uk)

Sitenin sahte olduğunun anlamadan siteye girdiğiniz bilgilerle zaten banka hesabınıza erişemiyorsunuz. Site "sitenin çok yoğun olduğu daha sonra tekrar denemeniz gerektiğini" bildiren bir mesaj veriyor. Ama o arada siteye girilen banka bilgileriniz çoktan dolandırıcının eline geçmiştir.

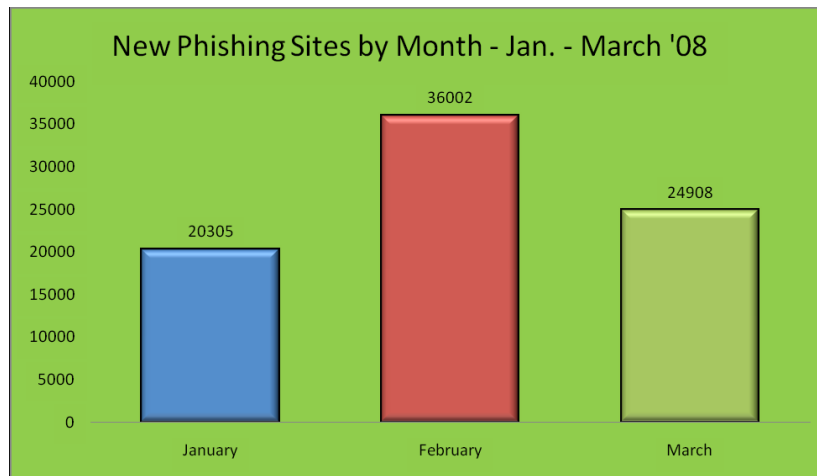
Burada yemlemeye gelmemek için dikkat edilecek husus bankanın hesap bilgileri ile ilgili olarak müşterilerine elektronik posta yolu ile kullanıcı bilgilerinin güncellenmesi için haber verip vermeyeceğinin bilinmesidir. HSBC Bank müşterilerine ait ayrıntılı bilgiler için elektronik posta göndermemektedir. Ayrıca girilen web sitenin tarayıcının adres çubuğu kısmına bakıldığında HSBC Bank'ın adresinin olmadığı görülecektir.

Aynı şekilde Akbank tarafından geliyormuş gibi görünen aşağıdaki elektronik postada verilen <https://www.akbank.com.tr> linkinin aslında <http://amdwebhost> ile başlayan web sitesi olduğu görülmektedir. Eğer bu şekilde gönderilen sahte web sitelerine girerseniz bankanızın çağrı merkezini aramanızda fayda vardır.



Şekil 4

Kimlik hırsızlığı ile mücadele eden bir organizasyon olan APWG(Anti-Phishing Çalışma Grubu) tarafından hazırlanan 2008 yılı ilk üç aylık raporunda tespit edilen phishing amaçlı sahte web sitelerinin sayısı Şekil-5' te görülmektedir. Buna göre Şubat 2008' te bir önceki aya göre %77'lik bir artış söz konusudur. Bu sitelerin barındıran ülkelerin başında ABD,Rusya ve Çin gelmektedir.



Şekil 5

Raporda ayrıca sahte sitelerin %99' unun 80 nolu porttan yayın yaptığı yani adreslerinin "http" ile başlayan siteler olduğu belirtilmiştir. Birçok kuruluşa ait web sitesi özellikle bankalara ait web sitelerinin adresleri bu durumdan korunmak için 443 nolu porttan hizmet verir yani adresleri "https" ile başlar. Yine rapora göre phishing sitelerinin ortalama %10' u bir IP numarası üzerinden çalışmaktadır ve bu sitelerin en uzun ömrü 30 gündür.

**b. Zararlı İçerikli siteler:** Zararlı siteler(malicious site) web tarayıcın exploitleri, zararlı javascript kodları ve ActiveX içerir. Bu siteler kullanıcıların bilgisayarına keylogger, Truva atı ve diğer casus programları yüklemek için zararlı programların adlarını kullanıcının dikkatini çekmek için değiştirirler. Örneğin sexygirl.exe, freemoney.exe gibi isimler vererek kullanıcıların dosyaları bilgisayarlarına indirip çalıştırmalarını sağlarlar. Burada phishing amaçlı kullanılan keyloggeer programlarını kısaca ele alacağız.

Keylogger programları bilgisayarınızda yaptığınız işlemleri, klavyede bastığınız tuşları, bilgisayarınızdaki ekran görüntülerini kayıt eden ve dolandırıcının belirlediği bir elektronik posta hesabına ya da bir ftp adresine gönderen casusu programlardır. İnternette indirdiğiniz çok masum görünen bir oyun programının içerisinde gizlenmiş bir casus program olabilir. Keylogger programı elektronik posta, sohbet programları ve bu amaçla hazırlanmış web siteleri yoluyla kurbanlarına gönderilir. Bu yolla bir web sitesinde girdiğinizde kullanıcı adları ve parolalar dolandırıcın eline geçebilir.

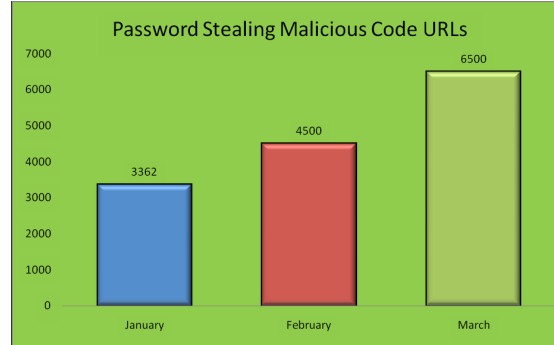
Klasik keyloggerlardan farklı olarak dolandırıcılık amaçlı keyloggerlarda hedef basılan her tuşu kontrol etmekten ziyade daha çok banka, elektronik alışveriş ve elektronik posta hizmeti veren web sitelerine girilen bilgileri ele geçirmektir. Bu amaçla hazırlanan keyloggerlar da önceki sayfalarda gösterilen Şekil-1' deki yöntemle çalışır.



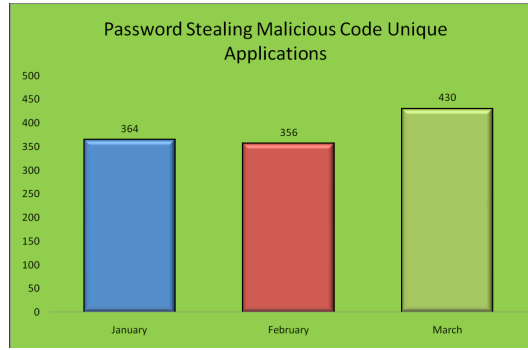
Şekil 6 <http://securitylabs.websense.com/content/Alerts/807.aspx>

Şekil6' da Websense Güvenlik Laboratuvarı' na rapor edilen bir elektronik posta mesajı içeriği görülmektedir. Mesajda görülen linke tıklandığında kullanıcı görüntülenmesi beklenen web sitesinde farklı olarak zararlı içeriği olan saldırı amaçlı bir web sitesine (malicious site) yönlendirilir.

Açılan web sitesi kullanıcının bilgisayarına gizlice casus programları indirir ve program çalışmaya başlar. Çalışan program bir bankacılık işlemi gerçekleştiğinde kullanıcıya ait bilgiler dolandırıcının belirlediği bir adrese gönderir. Dolandırıcılar kullanıcıları bu tip zararlı içerik barındıran sitelere yönlendirmek için erotik, arkadaşlık ve para konulu elektronik postalar gönderir. Torpig casus programı ile Kasım 2008' den bugüne kadar 500.00 adet kredi kartı, banka kartı ve debit kart çalınmıştır.



Şekil 7



Şekil 8

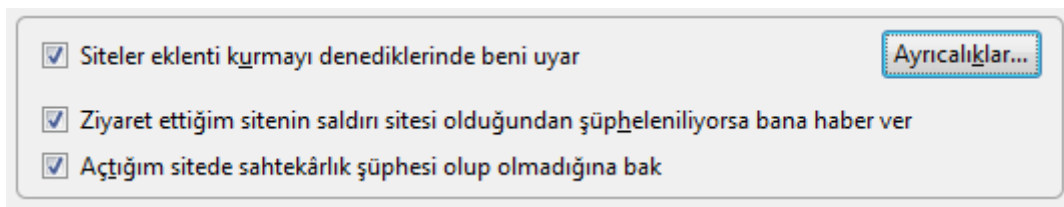
APWG raporuna göre dolandırıcılık amaçlı zararlı içerik barındıran web siteleri ile keylogger programlarının sayısındaki artış Şekil-7 ve Şekil-8' de görülmektedir. Bu amaçla hazırlanan web siteleri ve keylogger programları ABD,Çin ve Rusya tarafından hazırlanmaktadır.

### Web Tarayıcılarının Kullanımı

Web tarayıcıları bir web sitesinde yer alan sayfaları ziyaret etmemizi kolaylaştıran kullanıcı dostu arayüzlerdir. Web tarayıcıları web sitelerine erişmek için temel olarak "http" protokolünü kullanır. Bu sayede web sitelerinde bulunan yazı, resim,video ları web tarayıcıda görebiliriz. Web sitelerine web tarayıcılarına genellikle http ile başlayan URL bilgisini yazarak erişiriz. Örneğin <http://www.sayisaldelil.net> gibi. Burada http ile başlayan ifade bu sitenin URL' sidir. Bunun yanında bir çok kurum, alışveriş siteleri ve elektronik bankacılık hizmetlerinde web sitelerine erişmek için "https" yani güvenli http protokolünü kullanılır. Örneğin <https://sube.garanti.com.tr/isube/login>. Günümüzde en çok kullanılan web tarayıcıları Mozilla Firefox ve İnternet Explorer' dır. Bu iki web tarayıcısının phishing olaylarına karşı aldığı önlemleri inceleyelim.

#### a. Mozilla Firefox

Firefox , zararlı içerik barındıran web siteleri ile dolandırıcılık amaçlı hazırlanan web sitelerine karşı kullanıcıların güvenliğini artırmak için Firefox3 sürümünden itibaren on-line Phishing ve Malware (zararlı içerik) koruma özelliğini yayımlamıştır. Phishing ve Malware koruması, kullanıcıların ziyaret ettiği sayfalarla daha önceden Firefox' a rapor edilen zararlı içerik ve dolandırıcılık amaçlı sitelerin listesi kontrol edilerek çalışır. Web tarayıcısında bu özellik aktif ise her 30 dakikada bu listeler güncellenir.



Şekil 9

Firefoxtaki phishing koruması Google ve diğer partnerleri tarafından da desteklenmektedir. Firefox phishing ihbarlarını Google' a göndererek serverda bulunan karaliste ile karşılaştırır. Girilen phishing sitesi kara listede yer alıyorsa Firefox Şekil-10' daki i uyarıyı verir.



Şekil 10

Eğer girilen site zararlı içeriği olan bir site ise Şekil-11' deki uyarı verilir.



Şekil 11

(devam edecek)