

İnternet Korsanlarının Saldırı İçin Webi Kullanmalarının Nedenleri ve Önlemleri

10 NEDEN & 10 ÖNLEM

E-Siber.com

<http://www.e-siber.com>

10 SALDIRI NEDENİ

1. Masaüstünün Savunmasızlığı

Kullanıcılar sistemlerini her zaman yamamadıklarından ve sistemlerine gerekli güncellemeleri yapmadıklarından, İnternet Explorer, Firefox ve Windows işletim sistemi zararlı ve kötücül programlar için çok geniş bir ortam sağlıyor. Bazı kötücül niyetli programlar da kendiliğinden ilgili sistem ve programların açıklarını kullanarak kullanıcının izni olmadan kendini otomatik olarak sisteme yüklüyor.

2. Sunucu (server) Savunmasızlığı

İnternet Bilgi Sunucusu (Internet Information Server – ISS) ve Apache web sunucuları yamalanmamış sistemleri, varolan zayıflıkları ve sunucu yönetim ayar hataları nedeniyle bir diğer zengin saldırı hedef lerindedir.

3. Sanal (virtual) Sunucu Barındırma Hizmeti

Birçok hatta bazen yüzlerce sitenin aynı sunucuda barındırılması durumu da kötücül yazılımlar ve exploitleri için çok etkili bir hedef kaynağı olabilmektedir.

4. Açık Vekil Sunucular

Şu sıralar ülkemizde de oldukça meşhur bir yöntem olan yasaklı sitelere -DNS ve IP ayarlarını ilgili vekil sunucuya çevirterek- girme yolu olan vekil sunucular(proxy). Bu yolla bütün web trafiğiniz kimliği belirsiz ve ne amaçla kullanıldığı belli olmayan web sunucuları üzerinden iletilmekle beraber sisteminiz de bu sunuculardan gelebilecek kötücül programlar ve exploitlere açık olabilmektedir. Bütün web trafiğiniz de bu hat üzerinden gittiğinden mahremiyetinizin ve şahsi bilgilerinizin başka ellere geçme olasılığı oldukça yüksek.

5. HTML'nin Farklı Web İçeriklerini Gömme(Embed) Özelliği

Artık günümüzde birçok web sitesi farklı web kaynaklarındaki içerikleri kendi üzerinden yayınlamak için basitçe html embed diyebileceğimiz yöntemi kullanmakta. Bunu Google Analytics, reklam yayınlama networkleri, indirme(download) siteleri gibi popüler yerler sağladığı gibi ziyaret ettiğimizde kesinlikle kaynağını göremeyeceğimiz siteler de aynı yöntemi kullanmaktadır. Çok masum zannettiğimiz bir web sitesi belki böyle bir yerden içerik sağlıyor olabilir.

6. Her Kullanıcı Bir Güvenlik Uzmanı Değildir

Özellikle ülkemizde çoğu web kullanıcısı kişisel ve finansal bilgilerin girildiği network-ağ, bankacılık ve alışveriş gibi işlemler yapılan sitelerde SSL(Secure Socket Layer) yani "http://" yerine "https://" özelliğinin aranması, indirdikleri programların yasallığını kontrol etmeleri, güvenlik(firewall) duvarı kullanmaları, kimlik bilgisi çalan site ile yasal siteyi ayırt etmek ve bilgisayarları anormal davranışlar yaptığında neler yapması gerektiği bil(e)mez.

7. Mobil Kod Kullanımının Alabildiğine Yaygın Kullanımı

İnternete girdiğiniz web tarayıcınızda JavaScript, Java applets, .NET uygulamaları, Flash veya ActiveX gibi özelliklerin pasif hale getirmek kulağa son derece hoş geliyor olabilir. Fakat artık bunların kullanılmadığı web sitesi yok denecek kadar az. Bunların aktif olmadığı zaman girilen birçok web sitesi ya çalışmaz ya da açılmaz. Burada akla ilk gelen bunların bulunduğu sitelerin kodlamalarının bütün kurallara uygun olarak düzgün yapılması. Çünkü zayıf kodlama tekniklerinden kaynaklanan açıklar hem XSS(Cross-Site Scripting: Site Betik /Kod Çakışması)ye neden olmakta hemde kimlik ve iletişim bilgilerinin girildiği sitelerde zararlı kodlar aracılığıyla bilgilerin kolayca taşınabilmesine neden olabilmektedir.

8. Yaygın Genişband İnternet Kullanımı

Şirket güvenlik duvarlarının(firewall) çok güdü olmasına karşın, bağlantısında Ağ Adresi Dönüştürme(Network Address Translation -NAT) vb ağ özellikleri bulunmayan ev kullanıcılarının güvenlik duvarları kişisel bilgilerin toplanmasında ve

botnetlerde birer zombi bilgisayar olarak davranmalarına neden olabilir. Ve böylece botnet sunularındaki kötücül programların saldırısına açık bir hedef haline gelmeleri söz konusu olabilir.

9. HTTP ve HTTPS'ye Kapsamlı Erişim

Webi kullanmanın doğası gereği olarak internete erişim, bütün bilgisayarlarda HTTP(tcp port 80) ve HTTPS(tcp port 443) üzerinden gerçekleşir. Günümüzde sıkça kullanılan anlık mesajlaşma ve P2P programlarında bu portları özgürce kullanarak erişim sağlar. Tabiki bu kadar geniş port kullanım kolaylığı ve özgürlüğü beraberinde gerekli önlemlerin alınmaması sonucu korsan program ve uygulamalar açık kanal bırakabilmektedir.

10. HTML E-Posta Gönderiminin Benimsenmesi

SMTP'nin etkisi sayesinde hackerlar artık e-posta içine gömülü zararlı veriyi yerleştiremiyorlar. Onun yerine e-postanın içine şüpheli içeriği alıp getirecek sahte linkler ve bağlantılar yerleştiriyorlar. Bu bazen bir bankanın web adresi gibi görünebiliyor bazen de çok güvenilir bir web sitesinden geliyor izlenimine sahip bir e-posta adresi olabilir. Kullanıcı bağlantıyı/linki takip ettiği an zararlı ve kötücül içeriğe maruz kalabiliyor.

ALINABİLECEK 10 ÖNLEM

1. Mümkünse internete girerken bilgisayarınızın misafir hesabını kullanınız. Çünkü misafir hesabının birçok giriş ve çıkış yetkisi kısıtlandığı için virüslere ve kötücül yazılımlara karşı bayağı bir etkili olabilmektedir.
2. Herhangi bir web sitesine girmeden önce o sitenin güvenli olup olmadığından emin olmaya çalışın. Günümüzde kolay kolay hiçbir kimse/kurum size karşılığı olmadan bir program veya hediye vermez. Şüphelendiğiniz web adresini ziyaret etmeden önce www.e-siber.com/onlinetarama adresindeki online zararlı site tespit aracından geçirtip güvenli olup olmadığını öğrenebilirsiniz. Ayrıca artık Google da arama sonuçlarında zararlı ve saldırgan siteleri girilmesi tavsiye edilmez diye uyarıyor.
3. İşletim sisteminizin güncelleştirme ayarı sürekli otomatik modda kalmalıdır. Bunu kendinizin yapmayı denemesi birçok kez unutkanlıkla neticelenebilir.
4. Her canınızın sıkıldığı siteyi ziyaret etmemeniz şiddetle tavsiye edilemeyen bir anayasa haline gelmesine karşın hala ısrarla şüpheli bir siteye girmek istiyorsanız bilgisayarınızda çok güçlü bir virüs tarama yazılımı(ücretsiz olan [Avira Antivir Personal](#) çok etkili bir virüs koruma yazılımıdır.) kullanmanız, etkili bir firewall kumanız ve virüsten farklı kötücül ve casus programları için de bir casus tarama programı([Spyware Search & Destroy](#)) kullanmanız yüksek dozajda önerilir.
5. "Her gördüğün sakkalı deden zannetme!" örneğinden hareketle e-posta kutunuza ne idiği belirsiz kişi ve kaynaklardan düşen her e-postaya kanmamız ve geri iletişime geçmemiz ve dahi içindeki şüpheli bağlantıları "acaba nereye gidiyor " merak-ı saikiyle tıklayıp sonu hüsrarla neticelenen durumlarla karşılaşmamanız, internet çöplüğünde döne döne mevlevi posta haline gelmiş ve birbirine geçerek kördüğüm haline gelmiş zincir postalardaki şehir efsanelerine, mübareklik hurafelerine ve mazlum havadislerine kanmamamız için bir internet-bilgisayar okuryazarlığı kursu almanız ve bir süre bir uzmanın elinden geçmemiz şiddetle tavsiye olunur. Son zamanlarda artış gösteren bankalardan geliyor izlenimine sahip ve kişisel bilgilerinizi doldurmanızı isteyen hiçbir e-postaya güvenmemeniz konusunda neredeyse kanun hükmünde kararname olan resmi banka haberlerine itibar ediniz.

6. Herhangi bir bilgi ediniminde güvenli adresleri öğrenerek o kaynaklardan faydalanmak hem yanlış bir şeyler öğrenmenize mani olur hem de zararlı içeriklerle karşılaşmanızı önler.
7. Son yıllarda artan sosyal ağlara (facebook, orkut, hi5, power vb.) katılımınızı tekrar bir daha düşünerek bundan vazgeçmenizi şiddetle öneririz. Vazgeçemiyorsanız bile tanımadığınız ve hatırlamadığınız kimseyi ağınıza katmamanızı öneririz.
8. İnternet üzerinden gerçekte tanımadığınız biriyle “sanal bir ağ” üzerinden “sanal bir bağ” kurmayınız. İş ciddiye binebilir ve kendinizi karşı tarafta oluşturduğunuz izlenim üzerinden önlenemez vahim neticelerle başbaşa bulabilirsiniz.
9. İnternette resmi e-devlet ve bankacılık sayfaları dışında hiçbir yerde resmi bilgilerinizi girmeyiniz.
10. Güvenli olmayan şüphe uyandıran sitelerden program indirmeyiniz. İlgili programı ya sahibinin direkt web sitesinden indiriniz ya da www.download.com ve www.tucows.com gibi güvenilir indirme (download) sitelerinden indiriniz.