İNTERNET GÜVENLİĞİ

İnternet, çağımızda en hızlı iletişimi sağlayan, bilgi çeşitliliğini bir tuşla ayağımıza getiren bir ağdır. Peki bu harika ağda bizi bekleyen sadece güzellikler mi var? Hayır, gülün dikeni nasıl bir tehlikeyse internetin virüsü de bilgisayarımızın içinde depoladığımız (eczane programımız, resim-müzik vs. arşivlerimiz) yüzlerce bilgi için öldürücü bir dikendir.

VİRÜSLER

Bilgisayarınızın, sizin isteğiniz ve bilginiz dışında zararlı bir işlem yapmasını neden olan program parçacığına virüs denilmektedir. Günümüzde 100.000'e yakın virüs tespit edilmiş olup bu sayı sürekli artmaktadır. Virüsler yayılma yolu olarak genelde Windows işletim sistemlerinde otomatik olarak çalıştırılabilen dosya eklentilerini seçiyorlar.Yazılan her virüs tehlikeli değildir. Bir virüsün etkin halde olduğunu anlamak için birçok anti-virüs yazılımı sitesini gezip, bu sitelerin notlama sitemine göre yorum yapmak gerekmektedir

Virüslerin çeşitli bulaşma yolları vardır. İnternetin yaygın olmadığı zamanlarda disketlerle bulaşırlardı. İnternetle birlikte bulaşma riskleri oldukça arttı. İnternetten indirilen programlarla virüs kapabiliriz. Bu konuyu da yine kullanıcının bilinçli olarak indirdiği dosyalar ve kullandığı web-tarayıcısının (Internet Explorer, Netscape) otomatik olarak indirdiği dosyalar ile virüs bulaşması diye ikiye ayırabiliriz. Ya da icq, mirc gibi sohbet programları sırasında karşı taraftan aldığımız dosyalardan virüs kapabiliriz. Eğer bilgisayarımızı paylaşıma açmışsak ve bu paylaştırma sistemi yeterince güvenli değilse birçok kişi ağdan bilgisayarımıza girer ve dilediğini yapabilir. E-posta ile virüs bulaşması, e-postaların çalıştırılabilir eklentileri aracılığıyla olur. Virüsün aktif hale gelmesi için eklentileri açmamak her zaman bir koruma sağlamaz. Bazı e-posta okuyucu programlar belli formattaki eklentileri otomatik olarak çalıştırmaktadır.Esas kısmi kullanıcının sistem tarafından çalıştırılabilir dosyaları (.bat, .exe, .scr, .pif, vb) e-posta ile alması ve onu bilgisayarına çekmeden ya da çekerek çalıştırması ile sisteme virüs bulaştırmasıdır.

Truva Atı (trojan): Kendi kendine yayılmayan, arka planda çalışan program parçacıklarıdır Genellikle başka bir programa gömülü olarak gelirler. Örneğin bedava bir oyun programı buldunuz; ve yüklediniz. Böylece farkında olmadan oyun ile birlikte bir trojanı bilgisayarınıza kurmuş oldunuz. Program çalışmaya başladıktan sonra bilgisayara uzaktan erişimle kötü niyetli bir kişi istediği programı yüklemek, başka bilgisayarlara saldırmak gibi olanağa sahip olabilmektedir.

Makro Virüsler : Bunlar ofis uygulamalarında kullanılan belgelerin içine gömülü olan virüslerdir. Program veya komut çalıştırma yetkileri olduğundan çok tehlikeli olabilirler.

Hoax: Virüs olmadığı halde sistemimizdeki bir dosyanın virüs olduğu söyleyen yanıltıcı mesajlardır. Örnek vermek gerekirse;

Bir süre önce internette "sulfnbk.exe adlı çok tehlikeli bir virüsün silinmesi gerektiğine dair mesajlar bir anda milyonlarca kişiye ulaştı. Ve silenler bir sistem dosyasını silmiş oldular.

Virüsler ilk açılışta çalışmak için genellikle "Windows Registry" (kayıt) ayarlarını değiştiriler. Virüsler bulaştıkları bilgisayarın sistem kaynaklarını sömürerek yavaşlamasına hatta çökmesine, güvenlik açıkları oluşmasına yol açar. En önemli özellikleri ise adres defterine ulaşıp herkese kendisini bulaştırır. Bu yüzden bir virüs 2-3 gün içinde milyonlarca bilgisayara yayılabilir. Klişe bir deyimle "bir virüsün yapabilecekleri hayallerinizle sınırlıdır" diyelim ve de birkaç örnek verelim.

-Hard diske format (sabit diski tamamen silme) atabilir.

-Sistem dosyalarını bozar.

-Ekrana olmadık zamanlarda olmadık yazılar resimler çıkarırlar. . Bunlardan bir tanesi çok romantiktir. Ekrana zaman zaman "I love You" yazmaktadır.Tuşların yerini değiştirebilirler.

-Boot sektöre(bilgisayar ilk açıldığında bakılan yer) zarar verebilirler.

Peki bilgisayarımızda virüs olup olmadığını nasıl anlayabiliriz?

Bilgisayarımızın hızı oldukça yavaşlamışsa, işletim sistemi olmadık yer ve zamanda hata mesajları veriyorsa, programlarla ilgili saçma uyarılar çıkıyorsa, programların uzunluğu değişiyorsa, klavye tuşları zaman zaman hiç basmıyor ya da yanlış harf basıyorsa, bazı dosyalar kendiliğinden silinmişse, sistem kilitleniyorsa, bilgisayar takılı kalıyorsa, mouse kendiliğinden hareket ediyorsa, az evvel kaydettiğiniz belgede eksiklikler varsa ya belgede olmayan yazılar eklenmişse vs. Bunlardan bir kısmı dahi oluyorsa bile bilgisayarımızda bir virüs olma ihtimali vardır.

Bu durumda hiç telaşlanmadan yaptığımız işleri bitirip, kaydedeceğiz. Ve bilgisayarımızı kapatıp temiz bir sistem disketi ile açmalıyız, ardından bir anti virüs (bundan böyle AV olarak anılacaktır) programı ile sistemi taratmalıyız.

Nedir bu anti virüs programları ve de nasıl çalışırlar?

Adı üzerinde virüsleri yok etmeye ya da etkisiz hale getirmek amacıyla hazırlanan programlardır. AV programlarının veri bankasında birçok virüs kodu mevcuttur. AV programı kontrol ettiği belgede kendi bünyesindeki kodlardan birini bulursa o belgeyi virüslü olarak kabul eder. Buradan da anlaşılacağı gibi bir AV programının veri bankası ne kadar geniş ise virüs bulabilme ihtimali o kadar büyük olur. Peki bir AV programı yükledik. İş bitti mi? Elbette hayır. Çok bilinen bir tabirle tabirle "su uyur, düşman uyumaz". Virüs üreticileri sürekli yeni virüs yazarlar. AV program yaratıcı-ları da kendi programlarını yeni virüslere karşı sürekli geliştirler. Bu yüzden AV programını düzenli olarak internetten güncellemek gerekir. AV programı tarama yaptığımızda virüs bulaşmış dosyayı bize bildirir. Burada iki seçenek sunar. Onarma ve karantinaya alma. Onarmasını istediğimizde onarmaya çalışır.

Onaramamışsa karantinaya alır. Eğer ki o dosyanın işimize yaramayacak bir dosya olduğundan yüzde yüz eminsek silip kurtulabiliriz. Ama eğer kullandığımız bir programa aitse ve onarılamıyorsa orijinal programdan yeniden yüklemek en sağlıklı seçenektir.

Piyasada çeşitli AV programları vardır. Bunların birçoğu bir aylık deneme amacıyla ücretsizdir. Bir ay sonra satın alınmazsa kendiliklerinden işlevleri son bulur. Bunlardan en çok kullanılan birkaçının ismi ve web adresleri aşağıdadır.

Norton AV	www.symantec.com
Mcafee AV	www.mcafee.com
F-Prot AV	www.datafellows.com
Panda AV	www.pandasoftware.com/
Pc-cilin AV	www.trendmicro.com/en/home/global/enterprise.htm

Ama eğer ki ben para verip bir virüs programı satın almak istemiyorum diyorsanız :

www.symantec.com/avcenter adresine gidip sıra ile --->"check for security risk"-->"scan for virus" ;

www.mcafee.com adresinden —>"virusscan online" butonlarını tıklayarak hiçbir AV programı yüklemeden ücretsiz olarak online virüs taraması yaptırabiliriz.

FIREWALL

İnternete bağlı bilgisayarlar birbirileri ile iletişim kurarken "port"ları kullanırlar. Portlara bilgisayarların giriş kapıları da diyebiliriz. Web sayfalarına ulaşmak için http, e-posta için ise SMTP portları kullanılır. Kötü niyetli kimseler portscan denilen programlarla portları taratır ve eğer açık bulabilirse bu portlardan içeri girerek bilgisayarımızda dilediği işlemi yapabilir. Yapabilecekleri tamamen kişinin vicdanına kalmıştır diyebiliriz. Bunlardan en klasik ve masum olanı CDROM kapağını defalarca açılıp kapanmasıdır. Bu hareket muhtemelen bizi yerimizden sıçratacaktır. Biraz da komplo teorisine varacak örnekler verelim: Kişisel banka hesaplarınızı sizin adınıza kullanabilir, sizin bilgisayarınızı kullanarak bir başkasının banka hesabına illegal müdahale yapabilir. İşlemi sizin bilgisayarınız yaptığı için suçlu siz olursunuz.

Bunları Firewall diye bilinen programlarla engelleriz. Firewalllar ateş duvarı ya da güvenlik duvarı olarak nitelenebilir. Bu programlar bilgisayarın açık olan portları ile internet arasında durup içerden ya da dışarıdan istemediğimiz müdahaleleri engeller. Ayrıca saldırıda bulunan kişinin ip numarasını gösterdiği için karşı saldırı şansı da yaratır.Bu programlar virüs bulmaz. Ayrıca firewalllar özellikle Chat ortamlarında bilgisayarın kilitlenmesine neden olan nuke adlı programları engeller. En çok kullanılan firewall isimleri ve de web adresleri aşağıdadır.

BlackICE defender	http://blackice.iss.net/
Zone Alarm	www.zonelabs.com
eSafe Desktop	www.ealaddin.com
McAfee Firewall	www.mcafee-at-home.com
Norton firewall	www.symantec.com

Bunlar dışında güvenlik için ne yapmalı?

-Şifrelerimizi seçerken uzun ve tahmin edilmesi zor olan kelime ve sayı gruplarını büyük-küçük harf karıştırarak oluşturmalıyız. Mesela "Ne olursa olsun yaşamaya mecbursun" gibi bir şarkı sözlerinin ilk harfleri NooYM ve bunun sonuna da birkaç rakam konarak iyi bir şifre yaratalabilir. NooYM693 gibi.

-Mecbur olmadıkça bilgisayarı paylaşıma açmayın. Paylaşıma açmak şartsa uzun şifreler ile koruyun.

-www.windowsuptade.microsoft.com adresinden sistemimizi düzenli olarak güncellemeliyiz. Bu güncellemeler ile Microsoft kendi güvenlik açıklarını kapatmaktadır.

-Chat odalarında ve haber gruplarında gerçek adinizi kullanmayın hatta adinizi çağrıştıran takma adlardan da kaçının..

- Bir bedava e-mail hesabi edinip sizden e-mail isteyen yerlere onu verin, gerçek e-mail hesabinizi sadece dostlarınıza verin.

-Kişisel bilgi değişimi karsısında ödül veren sitelere kanmayın. Unutmayın verdiğiniz aldığınızdan daha değerli olmasaydı pesinizden koşarlar mıydı?

-Bedava mp3, program ya da porno sitelere girmeyin. Unutmayın her şeyin bir bedeli vardır.

-Zaman zaman denetim masasına bakarak bilginiz dışında yüklenmiş program varsa kaldırın.

-Düzenli olarak virüs taraması yaptırın. AV programını sık sık güncelleyin.

-Mutlaka bilgilerinizin bir yedeğini alın.

-Ofis programlarında bilmediğiniz makroları çalıştırmayın. Alternatif Office programlarına yönelin. Hem de ücretsizdir. Örneğin Open Office(www.openoffice.org)

Aşağıdaki ücretsiz programlar da bilgisayarımızdaki casus programları bulup yok ederler. Firewall ve AV programına ek olarak bilgisayarımızda bunların bulunması faydalı olur.

Ad-aware ----> http://www.lavasoftusa.com

SpyBot Search & Destroy—>http://security.kolla.de

Son olarak: Her adımınızın başkalarınca izlendiği bir dünya hayal edebiliyor musunuz? Nereye giderseniz gidin nereye bakarsanız bakın ve kiminle ne görüşürseniz görüsün hepsi izleniyor. George Orwell'in kitabında bahsettiği "Big Brother" ya da "Truman Show"adlı filmede işlenen teoriler maalesef günümüzde gerçeğe dönüştü. Şöyle ki: İnternette dolaşırken, mail yollarken, telefonla konuşurken, faks çekerken, cep telefonundan mesaj gönderirken oluyor. Amerika'nın kurduğu "ECHELON" adı verilen ve düşünemeyeceğimiz kadar büyük, devasa işlem hacmine sahip bir bilgisayarlar ağı tüm iletişim sistemlerini tarıyor. Ve kendisine verilen anahtar sözcük, sayı, şifre her ne ise bulduğu anda kayıt yapmaya başlıyor. Unutmayın : "BİRİ BİZİ HER AN İZLİYOR".

Yayına Hazırlayan
Ecz Ali ÇEVRİM
4. Bölge Adana Eczacı Odası
Bilgisayar Komisyonu Üyesi