GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

ARALIK 2016

Aman Cebimize Mikrop Girmesin...

ÇAĞIMIZIN TEKNOLOJİK OLANAKLARI, BİR YANDAN YAŞAMIMIZI KOLAYLAŞTIRIRKEN, DİĞER YANDAN BERABERİNDE ÇEŞİTLİ RİSKLER GETİRİYOR. Mobil cihazlar yediden yetmişe herkesin tutkusu haline geldi. Bunun bir nedeni teknolojiyi gittiğimiz her yere taşıma arzumuzsa, bir nedeni de cihazların rengârenk, anlaşılır, bir dokunuşla kolaylıkla komuta edebildiğimiz cazip arayüzlere sahip olması.

Artık gün geçmiyor ki "post"larımızın, "tweet"lerimizin altında sevgili annelerimizin, teyzelerimizin, halalarımızın tatlı yorumlarını görmeyelim. Çocuklarımız ise bizlerden çok daha hızlı ve rahat kullanıyorlar bu cihazları. Arkadaşlarıyla mesajlaşmalar; delikanlılar arasında klanlar kurmalar, kaleler yapmalar, saldırı ve savunma stratejileri geliştirmeler; küçük hanımefendiler arasında ise modacı halleriyle kıyafetler, saçlar başlar tasarlamalar, ahçı halleriyle malzemeleri karıştırıp çeşit çeşit sanal yemekler hazırlamalar, "pet"ler edinip beslemeler, taramalar, süslemeler; ayrıca şarkılar söyleyip videolar çekmeler ve daha neler neler... Saymakla bitmez... Bizde iki modelden de mevcut, anlamışsınızdır belki de okurken.

Hal buyken, o janjanlı uygulamaların cazibesi içinde, çeşitli virüsleri de kendi ellerimizle bu cihazlara yükleme tuzağına düşmemiz çok olası.

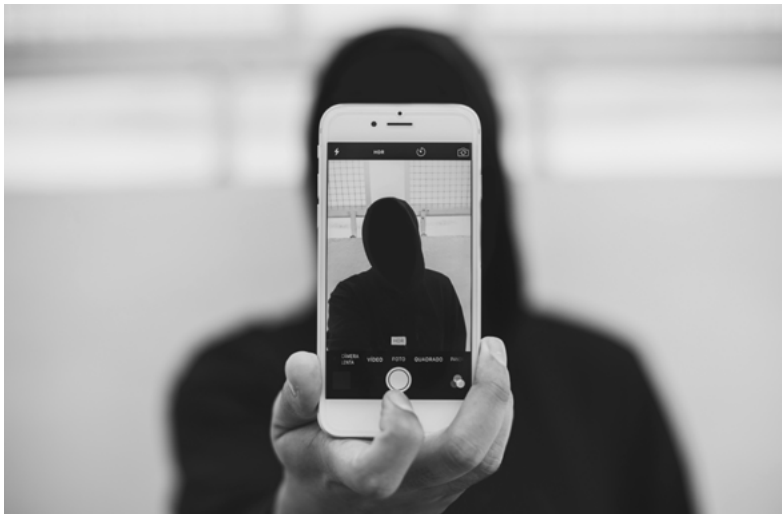
Bu virüsler neden var? Cihazlarımızın üzerinde neler yapıyorlar?

Virüslerin varlıklarının da çeşitli nedenleri var. Bazıları cihazımıza uzaktan komuta edilmesini sağlayarak bize gelen ya da giden SMS'leri istenen bir başka sistem üzerine aktarabiliyor, kendi başına SMS gönderebiliyor, gelen SMS'leri yanıtlayabiliyor, gelen çağrıları bir başka sistem üzerine aktarabiliyor ya da yanıtlayabiliyor, bizim numaramızdan arama yapılabiliyor. Bazıları ise dedektif, hatta casus gibi çalışarak kurulduğu telefondan yapılan konuşmaları ya da telefonun bulunduğu ortamı dinleyebiliyor, başka numaralara yönlendirmeler yapabiliyor. WhatsApp, Skype, Viber, Facebook, Messenger gibi anlık sohbet uygulamalarında neler yazıştığınızı harfi harfine görüntüleyebiliyor ve sosyal ağların takibini sağlayabiliyor. Bu gibi yazılımlarla metin mesaj takibinin yanı sıra e-posta, internet kullanımı, arama kaydı ve GPS üzerinden konum belirleme gibi farklı takipler yapmak da mümkün.

Diğer nedenler arasındaysa, görece masum sayılabilecek bir bölümünün sizi reklam bombardımanına tutabilmesi ya da daha da vahimi cihazınızın bir saldırı ordusunun askeri haline getirilebilmesi sayılabilir. Böylelikle çeşitli kurum ya da sistemleri hedef alarak yapacakları siber saldırılarda sizin cihazınızın gücünü de kullanabilirler. "Aman benim cücük kadar cihazımın gücünden ne olur ki" demeyin; binlercesi, on binlercesi, yüz binlercesi, hatta milyonlarcası bir araya geldiğinde çok şeyler oluyor. Aygıtlarca internet (IoT) kullanımı yaygınlaştıkça buzdolabınızın bile ummadığınız kötülükteki işlerin bir parçası haline gelmesi mümkündür! Neyse, konumuzu dağıtmadan devam edelim dilerseniz.

Peki cihazınızda virüs olup olmadığını nasıl anlarsınız?

Farklı amaçlarla hazırlanmış olan çeşitli virüsler mobil cihazlar üzerinde farklı etkiler yaratabiliyor. Örneğin cihaz üzerinde yaptığınız işlemleri kaydedip farklı sistemlere yönlendiren virüsler genel olarak cihazın daha yavaş çalışmasına yol açıyor. Reklam bombardımanı yapanları zaten fark etmemek mümkün değil. Cihazınızı "zombie" diye de tabir edilen, kendi saldırı ordularının askeri haline getiren virüsler ise cihazı neredeyse kullanılamayacak duruma getirip, donup kalmasına neden oluyorlar.



Anladık ki cihazımızda virüs var ama silemedik. Şimdi ne yapacağız? Nasıl kurtulacağız?

Öncelikle güvenilir bir antivirüs yazılımı indirerek cihazı taratabilir ve bulunan zararlı yazılımları kaldırabilirsiniz. Burada dikkat edilmesi gereken bir nokta, cihazda kullanacağınız antivirüs yazılımını cihazınızın kendi uygulama marketinden indirmeniz. Bir başka önemli nokta da, indireceğiniz antivirüs yazılımının güvenilir olmasını sağlamanız. Aksi durumda kaş yapayım darken göz çıkarabilirsiniz. Antivirüs niyetiyle cihazınıza yüklediğiniz yazılım, başınıza daha büyük dertler açacak bir başka virüs yazılımı olabilir. Güvenilir sayabileceğimiz yazılımlar arasında bu alanda kendini kanıtlamış olan Avast, Avira ve Norton sıralanabilir.

Bizi bu aşamada da çaresiz bırakabilecek diğer bir nokta da, virüs yazılımlarının, kendilerini sistemin bir parçası gibi göstererek, antivirüs yazılımları tarafından kaldırmalarına izin vermeyebilmeleridir.

Antivirüs de işe yaramadıysa ne yapmalı, ne etmeli?

Zararlı yazılımlar genellikle Android platformları için üretilmekte olduğundan, birçok Android cihazda desteklenen "Güvenli Mod"a geçiş yapabilirsiniz. Cihaz bu modda açıldıktan sonra, sonradan yüklenen uygulamalar pasif hale gelmekte ve kaldırmanız mümkün olabilmektedir. Bu moda geçiş için telefonunuzun markasını ve model numaranızı belirterek yapacağınız bir Google aramasıyla kendi cihazınız için geçerli olan yöntemi bulabilirsiniz.

Eyvah, yine olmadı, ne olacak şimdi?

Bu noktada telefonunuzda bulunan fotoğraf, notlar, ses kaydı, mesajlar ve diğer verilerinizi bulut ya da PC'nize yedeklediğinizi umarak devam edelim. Ne yazık ki kurtuluş için cihazınızı önce sıfırlamanız ve sonra yeniden kurmanız gerekir. Bu işlemle cihazınızdaki bütün verileriniz de sıfırlanmış olacaktır haliyle. Buraya kadar geldiyseniz, bu kez cihazınızı yeniden kurduktan sonra ilk indireceğiniz uygulama, güvenilir bir antivirüs yazılımı olsun derim. Daha sonra kullanmaya alışık olduğunuz ve kaynağını güvenilir bulduğunuz diğer ek uygulamaları yüklemeye devam edebilirsiniz.

Peki bu duruma hiç düşmemek için ne yapmalıydık?

Cihazımız "jailbreak", yani diğer bir deyişle "kırılmış" bir cihaz olmamalıdır. Normal koşullarda üreticiler, sizin için risk yaratacak, güvenilir bulunmayan yazılımların cihazlara yüklenmesine izin vermezler. Ancak kırılmış olan /jailbreak işleminden geçmiş olan telefonlarda üreticinin bu kontrolü devre dışı kalıyor.

Cihazımıza kendi uygulama marketi dışında bir kaynaktan herhangi bir yazılım yüklemememizde de yarar var. Cihazımızın üzerine kuracağımız tüm yazılımların güvenilir olduğundan emin olmalıyız.

Yazılım kurarken cihazınız birçok aşamada sizden yapacağı işlemler için onay isteyecektir. Örneğin kameraya erişsin mi, fotoğraflarınıza erişsin mi, lokasyonunuza erişsin mi gibi sorular sonacaktır. Bu soruları geçiştirmeden dikkatle okumanızı ve erişim talep eden servislerin kurduğunuz yazılımın amacıyla ilişkili olmaması halinde izin vermemenizi öneririm.

Herkese virüssüz, mikropsuz, sağlıklı, güzel günler olsun.

YAZAR HAKKINDA

Ayşim Niksarli, 1992'da İTÜ Elektronik Mühendisliği'nden mezun olarak iş yaşamına adım atmıştır. 24 yıllık sektör deneyiminin son 16 yılında finans kurumlarında Bilgi Güvenliği Yöneticiliği yapmıştır. ISC2 Türkiye Chapter kurucu üyesidir. Gönüllü profesyonel koçluk ve mentorluk da yapmaktadır.