turk.internet.com™

Mert Sarıca : Kullanıcıların Cep Telefonlarında Yüklü Uygulamaların İzinlerini Kontrol Etmesi Ya da Arasıra Fabrika Ayarlarına Dönmesi İyi Olur

Fusun S.Nebil - fusun@nebil.com
28 18:00:00-03-2016

Çeşitli haberlerimizde, bilgisayarlarımıza habersizce sızan, sızdırılan virüs ve trojanların neler yaptığını anlatıyoruz. Bunlar bize ait verileri çalabildikleri gibi, bilgisayarlarımızı bir dDOS saldırı aracı ya da bir yerlerde yazı, sayfa ya da reklam tıklar, beğenir hale getirebiliyorlar.

Bu nedenle turk-internet.com olarak, önem verdiğimiz konuların başında "Siber ve Mobil Güvenlik" geliyor. Hatta mobil güvenlik bugün, çok daha önemli bir hale geldi. Çünkü elimizdeki küçücük aletler, artık her türlü işimizi ve özel hayatımızı sürdürme aracı haline geldi. O nedenle de, cep telefonlarını kullanırken siber güvenlik risklerini de farkında olmamız gerekli.

Bu konularda farklı kaynak ve uzmanlardan aldığımız bilgileri, haberleri ya da söyleşileri yayınlamayı sürdüreceğiz. Bunlardan birisi Bahçeşehir Üniversitesinde Yüksek Lisans Programlarında ders veren Mert Sarıca. Kendisiyle mobil güvenlik konusunda görüştük;

turk-internet.com : Kendinizi tanıtır mısınız?

Mert Sarıca : Kariyer hayatım, 2003 yılında eğitim aldığım üniversitenin elektronik ders seçme uygulaması üzerinde keşfetmiş olduğum kritik güvenlik zafiyetini üniversite yönetimi ile paylaşmam ile başladı. Bu paylaşım üzerine üniversite yönetimi tarafından başarı bursu ile ödüllendirildim ve 2005 yılında Ethical Hacker olarak işe alındım. 2006 yılında Yeditepe Üniversitesi, Bilişim Sistemleri ve Teknolojileri bölümünden mezun oldum. 2010 yılında ise Yeditepe Üniversitesi, İngilizce İşletme (MBA) programını tamamladım.

2007 yılından bu yana Finansbank'ın Bilgi Teknolojileri firması olan IBTech firmasında Expert Penetration Tester / Ethical Hacker olarak çalışmaktayım. Penetrasyon testinin yanı sıra zararlı yazılım analizi ve tersine mühendislik alanlarında da uzmanlaşmaktayım.

2014 yılı itibariyle Bahçeşehir Üniversitesi, Siber Güvenlik Yüksek Lisans Programı'nda Zararlı Yazılım Analizi dersi vermekteyim.

Boş vakitlerimi bilişim güvenliği üzerine araştırmalar yaparak ve kişisel web sitem olan mertsarica.com adresinde yayımlayarak geçirmekteyim.

turk-internet.com : Hep firmalara, bankalara ya da devlete yapılan siber saldırıları konuşuyoruz ama gelişen teknoloji sayesinde, bireyler de otobüslerde ya da günlük hayatta siber saldırıların hedefi olabilir deniliyor. Cep telefonlarımız konusunda hangi tehlikeler var anlatabilir misiniz?

Mert Sarıca : Aslında akıllı telefonlar hayatımıza girdi gireli, son kullanıcılar olarak tehditlere çok daha açık hale gelmeye başladık. Bunun başlıca sebeplerinden birisi olarak, mobil platformlar için geliştirilen işletim sistemlerinin masaüstü/sunucu işletim sistemlerine kıyasla (biraz da performans kaygılarından ötürü) daha az güvenlik özellikleri barındırması olduğunu söyleyebiliriz.

Özellikle Android işletim sistemi özelinde konuşacak olursak, yüklenecek uygulamanın hangi verilere ulaşacağı kararının son kullanıcıya bırakılması ve işletim sisteminin güvenlik yamalarının yüklenebilmesi için işletim sistemi geliştiricisinin dışında bir de cihaz üreticisinin yamayı dağıtmasını beklemek birçok kullanıcıyı uzun bir süre tehditlere açık hale getirmektedir.

Örneğin bundan birkaç yıl önce, masaüstü işletim sistemlerini hedef alan ve ülkemizde de oldukça yaygın olan internet bankacılığı zararlı yazılımları (Zeus, SpyEye, Hesperbot vb.), yerlerini Android platformunda çalışan mobil bankacılık zararlı yazılımlarına (Slempo/SlemBunk) bıraktı.

Yeri gelmişken bankada çalışan bir güvenlik uzmanı olarak, sizin sayesinde farkındalığı arttırma adına bu zararlı

yazılımın nasıl çalıştığını ve son kullanıcılar tarafından nasıl tespit edilebileceğine de kısaca dikkat çekmek isterim.

Ülkemizde sıklıkla görülen bu zararlı yazılım türü, kullanıcı tarafından yüklendikten sonra kendisini cihaz yöneticilerine (device administrators) ekleyerek, bankanın mobil bankacılık uygulaması çalıştırıldıktan hemen sonra kullanıcının ekranına sahte bir form çıkarmaktadır. Bu form sayesinde kullanıcının mobil bankacılık kullanıcı adı ve şifresini çaldıktan sonra banka tarafından gönderilen tek kullanımlık SMS doğrulama kodunu da sistem üzerinden çalarak, kullanıcının haberi olmadan dolandırıcıların kullanıcının bankacılık hesabına ulaşmasına imkan tanımaktadır.

Cihaz yöneticileri kısmında Flash Player adı altında yer alan bu zararlı yazılıma rastlanılması durumunda kullanıcıların en kısa sürede bankaları ile iletişime geçmelerini öneririm.

turk-internet.com : Genel anlamda Nasıl Korunmalıyız?

Mert Sarıca : Akıllı cihazlarımızın/telefonlarımızın masaüstü sistemlerimiz kadar belki daha da fazla tehditlere açık olduğunu unutmamamız gerekiyor. Bugün bakıldığında antivirüs yazılımı yüklü olmayan masaüstü/dizüstü bilgisayar neredeyse oldukça az ancak konu akıllı cihazlara geldiğinde, performans ve şarj süreleri nedeniyle güvenlik uygulamalarını bu cihazlara yüklemekten çoğunlukla kaçınıyoruz.

Halbuki akıllı cihazlar üzerinden alışverişten, bankacılık işlemlerine, e-posta okumaktan telefon görüşmelerine kadar, gün içinde ihtiyaç duyduğumuz tüm ihtiyaçlarımızı gerçekleştiriyoruz. Durum böyle olunca da aslında hem kişisel hem de kurumsal, bizim için hassas olarak verilerimizin bu cihazlar üzerinde olduğunu kimi zaman unutabiliyoruz. Biraz klişe de olsa, masaüstü/dizüstü bilgisayarlarımızda olduğu gibi akıllı cihazlarımıza da güvenlik uygulamaları yüklememiz gerektiğini söylemeden geçmek istemiyorum.

Örneğin eskiden aptal olan ancak akıllandıkça sesli komut alabilen (ortam sesini dinleme özelliği), kamerası olan akıllı televizyonumuza bir zararlı yazılım bulaştığında başımıza gelecekleri kestirmesi güç değil. Sahip olduğumuz cihazların akıllandıkça, kötü niyetli kişiler tarafından akıllı casuslara dönüştürülebileceğini asla unutmamalıyız.

turk-internet.com : Tekrar başa dönersek, diyorsunuz ki; *"Android'de yüklenecek uygulamanın hangi verilere ulaşacağı kararının son kullanıcıya bırakılması.."* Bunu biraz daha acalim.. Bu neden sorundur ve de bu soruna karşı kullanıcı ne yapmalı? Yani neye ve nasıl dikkat etmeli?

Mert Sarıca : Bildiğiniz üzere güvenlik farkındalığı hem son kullanıcılar hem de kurumsal kullanıcılar için büyük bir sorun. Bugün sahte fatura başlığı ile e-posta kutunuza gelen bir e-postada yer alan bağlantı adresine (link) tıkladığınızda, tüm verileriniz zararlı yazılımlar tarafından şifrelenebiliyor ve eliniz, kolunuz bağlı, verileriniz karşılığında dolandırıcıların istediği fidyeyi ödemek zorunda kalabiliyorsunuz.

Kurumları hacklemek isteyen art niyetli kişiler ise bugün birbirinden farklı güvenlik cihazları tarafından korunan sistemleri hedef almak yerine en zayıf halka olan kullanıcıları hedef alıyorlar. Kullanıcıyı kandırmanın, korunaklı sunucuları hacklemekten çok daha kolay olduğunu bildikleri için kurumlara bu şekilde sızabiliyorlar. Kısaca bilgi güvenliğinde en zayıf halka olan güvenlik farkındalığı düşük bir kullanıcıya, güvenliği ile ilgili karar aldırmak kullanıcıyı istemeden de olsa zor durumda bırakabiliyor.

Örneğin Google Play'den bir oyun indiren Android kullanıcısı, oyunu yüklerken karşısına çıkan onay ekranında oyunun hangi kişisel verilere ulaşacağına dikkat etmez ise, oyun adı altında yayılan bir zararlı yazılım rehberinizi ve smslerinizi çalabiliyor. Burada kullanıcının yükleyeceği uygulamanın cihaz üzerinde nelere erişmek istediğini dikkatlice kontrol etmesi gerekiyor.

turk-internet.com : Mobil işletim sistemlerinde güvenlik nasıl?

Mert Sarıca : Eskiye kıyasla iyiye doğru gittiğini söyleyebiliriz ancak cihazların üretici kaynaklı nedenlerden dolayı güncelleme almakta gecikmesi, kullanılan işletim sistemlerinin desteğinin üretici tarafından kesilmesi, uzun yıllar aynı cihazı kullanan akıllı cihaz kullanıcılarını risk altında bırakıyor. Modern Windows ve Linux işletim sistemlerinde yer alan güvenlik önlemlerinin mobil işletim sistemlerine adapte edilmesi yavaş olduğu için (Örnek işletim sistemi bazında ASLR kullanımı ve tarihleri: wikipedia/../Address Space Layout Randomization), modern saldırılara karşı kullanıcıları zor durumda bırakabiliyor.

turk-internet.com : Kullanıcılara tavsiyeniz nedir? Hangi yazılımı yüklediklerine, bir şeyden şikayet ettiklerinde mi, düzenli olarak mı bakmalarını tavsiye ediyorsunuz? Bunu da açalım. Nasıl yapacaklar?

Mert Sarıca : Aslında yanlış bilgilendirmeler nedeniyle kullanıcılar çoğunlukla cihazları yavaşladığında, cihazlarının şarjı hızla azalmaya başladığında casus bir yazılım olduğu endişesine kapılıyorlar. Halbuki bu gibi

durumlar haricinde de, cihazlarında bir yavaşlık olmadan, şarjları azalmadan da zararlı yazılımın kontrolü altında cihazlarını kullanıyor olabilirler. En azından Android mobil bankacılık zararlı yazılımlarına karşı kullanıcıların cihaz yöneticileri kısmını zaman zaman kontrol etmelerini tavsiye edebilirim. Zararlı bir uygulamayı yüklediğinizde bu uygulama ikonunu gizleyebildiği için kullanıcıların mutlaka bir güvenlik uygulaması yükleyerek cihazlarını bu gibi bilinen tehditlere karşı en azından koruma altına almalarını önerebilirim.

turk-internet.com : Teknik bir dolandırıcılık değilse de, Bir başka dolandırıcılık yöntemi, mobil telefon kullanıcısının dolaştığı sayfalardaki bir alanda bulunduğu için yüklenen yazılımlar. Mesela bir süre önce Joliess yazılımı konuşuldu (Bkz : Mobil Dolandırıcılara Dikkat ; Joliess İsteğiniz Dışında Ücretli Abone Yapıyor).. Bu tür olaylara karşı ne tavsiye edersiniz?

Mert Sarıca : Belirttiğiniz gibi teknik olmadığı için kullanıcılara operatör üzerinden mobil ödemeyi kapattırmalarını tavsiye edebilirim.

turk-internet.com : Bahsettiğiniz bankacılık sahte formu ya da fidye yazılımı konusunda rastlandığı üzere, tıklandığında virüs/trojan yükleyen çeşitli phishing mailleri, siteleri görülüyor. Bunları nasıl ayırdedeceğiz. Neye bakacağız? Nasıl önlem alacağız?

Mert Sarıca : Dolandırıcılar son zamanlarda kullanıcıları korkutarak, endişeye sevk ederek veya ikna yolu ile zararlı yazılımları/uygulamaları çalıştırmaya zorlamaktalar. İzledikleri yöntemler oldukça gerçekçi olduğu için teknik olarak kullanıcıların bunu gerçeğinden ayırt etmeleri güç olabilir bu nedenle burada en önemli nokta kullanıcının soğuk kanlı bir şekilde ilgili yerlerle iletişime geçmesi olacaktır. Örneğin beklemediği bir anda e-posta kutusununda 1.000 TL tutarında ödenmemiş fatura bulan bir kişinin yapması gereken ilk iş, ekte yer alan dosyayı veya e-postada yer alan bağlantı adresine (link) tıklamadan önce hizmet aldığı firmayı aramak olacaktır aksi durumlarda dolandırıcıların ağına düşebilirler.

turk-internet.com : Kendi cep telefonlarımızın casus hale dönüşmesini nasıl kontrol altına alabiliriz. Örneğin kamerasının kontrolünün başka bir yere geçip geçmediği nasıl anlaşılır? Ya da ortam dinlemesi için kullanılabilir mi?

Mert Sarıca : Bildiğiniz üzere geçtiğimiz yıl devletler için casus yazılım geliştiren bir firma hacklendi ve tüm e-posta yazışmaları sızdırıldı. Güvenlik firmalarının ve araştırmacılarının sızan bu e-postalar üzerinde yapmış oldukları araştırmada, bu firmanın geliştirmiş olduğu mobil uygulama ile hedef akıllı telefonun mikrofonunun dinlenmesi, sms, mms mesajlarının izlenmesi, kamera üzerinden fotoğraf çekilebilmesinin mümkün olduğu görülmektedir. Bu konuda endişe duyan kullanıcılar, yüklü uygulamaların izinlerini kontrol edebilir (mikrofona ve kameraya erişimi olan uygulamalar), belli zamanlarda telefonlarını fabrika ayarına çevirebilir, kontrolü altında olan bir kablosuz ağ (sim kartı çıkartmalıdır) ve proxy sunucu üzerinden internete çıkararak bağlantılarını izleyerek telefonunun nerelerle haberleştiğini kontrol edebilirler.

turk-internet.com : Enfekte olmuş bir mobil cihaz, başka cihazlara trojan bulaştırmak için kullanılabilir mi? Ya da tam tersi mümkün mü? Bu nasıl bir tehlike yaratabilir?

Mert Sarıca : Aslında bunun aynı ağda bulunduğunuz ve enfekte olmuş bir cihazın oluşturacağı tehditten bir farkı bulunmuyor. Şayet enfekte olmuş ve uzaktan yönetilen cihazda art niyetli kişi root yetkisine sahip ise, örneğin aynı ağda yer alan cihazlara ortadaki adam saldırısı (MITM) gerçekleştirerek trafiğini manipüle etmeye çalışabilir ve diğer sistemlere zararlı yazılım yükletmek için farklı yöntemler izleyebilir. Burada sınırlar, yöntemler, işletim sisteminde çalıştırılabilecek yazılımların becerileri ile sınırlı olacağı için ağ için büyük bir tehdit haline gelebilir. Bu durumu benzer bir şekilde iş yerine cihazını getirip, bağlayan personelin yaratacağı risk ile de özdeştirebiliriz.

turk-internet.com : Mobil telefonumuzun kullanmadığımız zamanlarda bile pilinin tükenmesi ya da ısınmış olması, bir şeye işaret eder mi? Bu durumda ne yapmalıyız?

Mert Sarıca : Yeni bir telefon almanıza işaret edebilir :) Şaka bir yana 8 çekirdekli işlemciye ve 4 GB RAM'e sahip olan cihazlarda bilgilerinizi çalıp, komuta kontrol merkezine gönderen bir uygulamanın cihazınızda performans sıkıntısı yaratmasını ben düşük bir olasılık olarak görüyorum. Yine de bu gibi durumlarda endişe duyan kullanıcılar, sistemlerini fabrika ayarlarına geri döndürebilirler.

turk-internet.com : Ücretsiz ya da genel wifi alanları cep telefonları için risk taşır mı?

Mert Sarıca : Kesinlikle. Bu konuya dikkat çekme adına geçtiğimiz yıl oldukça güzel bir çalışmaya imza atmıştım. Detaylarını merak edenler burayı tıklayarak okuyabilirler.

turk-internet.com : Son Apple-FBI olayında, Apple cep telefonunarına şifre olmaksızın girilemediğini gördük. Sonradan FBI başka bir çözüm bulduğunu söyledi. Bu olayı nasıl değerlendiriyorsunuz..

Mert Sarıca : Bunu kedi fare oyunundan farksız görmüyorum. Sonuçta yazılımların ve donanımların hataları olabilir ve güvenlik araştırmacıları, güvenlik firmaları bu hataları, farkındalığı arttırma adına kamuoyu ile paylaşabildiği gibi ticari bir fırsata da çevirebilir. Bir güvenlik uzmanı olarak şu çok güvenli, bu çok güvensiz gibi çıkarımlarda bulunmaktan ziyade her sisteme güvensiz olarak yaklaşmayı tercih ediyorum. Edward Snowden gizli belgeleri yayınlayana dek belki de çoğumuz NSA'in yapabileceklerinin sadece hayalden ibaret olduğunu düşünüyordu ancak gerçekler çoğu kimseyi yanılttı. Sanmıyorum ki hiç bir istihbarat servisi (NSA gibi), kamuoyuna yansımış bir dava için elindeki gücü kolayca harcasın. (FBI ile paylaşım) :)