

COMODO

Creating Trust Online®

Comodo: Pokemon Go işinizi tehdit etmesin

COMODO, 15.08.2016 - Bilişim dünyası, hayranlarına her gün yenileri eklenen internet oyunu Pokemon Go'nun yarattığı güvenlik sorunlarına çözüm ararken, Comodo'dan da uyarı geldi. Siber dünyada sunduğu güvenlik garantisi ile dikkat çeken Comodo, hem mobil hem de masaüstü platformlarda cihaz ve veri güvenliği sağlayabiliyor.

Comodo'nun Pokemon Go'nun yarattığı güvenlik açıklarıyla ilgili süren tartışmaları yakından izlerken yaptığı tespit kurumsal verileri de ilgilendiriyor. Öyle ki; Türkiye dahil pek çok ülkede henüz resmi olarak satışa sunulmayan Pokemon Go için yüzlerce resmi olmayan uygulama var. Google Play ve Apple Store dışındaki site ve uygulama dükkanlarından yüklenen uygulamalarda güvenlik açıkları dikkat çekiyor. Bu güvenlik açıkları kişilerin iş bilgileri için de önemli riskler oluşturuyor. Çünkü uygulamalar, yüklenmeden önce geniş erişim izinleri istiyor. Böylelikle, telefonunuzdaki bazı bilgilere erişim olanağı sağlarken telefonunu iş amaçlı da kullanımında risk yaratıyor. Bu noktada Comodo; "mobil cihazlara dikkat" diyor:

- Mobil cihazlar geleneksel olarak en az korunan cihazlar olarak biliniyor. Bunun nedeni de kullanıcıların çoğu zaman güvenlik tedbirlerini baypas etmesi. Bu durum; birçok şirkette, çalışanların mobil cihazlarıyla şirket ağına ve iş açısından kritik öneme sahip verilere erişmesinin yolunu açıyor. Çalışanlarının mobil cihazlarını iş için kullandığı durumlarda şirketlerin '**Mobil Cihaz Yönetimi**' uygulamalarını kullanmaları, çalışanlara ait mobil cihazlar bakımından güvenliği sağlamak ve iş verilerini korumak için en iyi yöntem olarak öne çıkıyor.
- Pokemon gibi güvenlik konusunda dolandırıcılık uygulamaları örnek olarak alındığında, mobil cihaz yönetimi çözümleri cihazı uzaktan kilitleme ve cihaz içeriğini tamamen silme yeteneğini gösteriyor. Kullanılan çözüme bağlı olarak 'admin'ler bir cihazın içeriğinde belirledikleri bilgilerin tamamını veya bir kısmını silebiliyor.
- Mobil cihaz yönetim çözümleri aynı zamanda cihazlarında yüklü olan güvenlik önlemlerini baypaslayan çalışanlara karşı da yöneticilere yardımcı oluyor. Sürekli izleme özellikleri sayesinde yöneticiler cihazların şirket tarafından belirlenen güvenlik politikalarına her zaman uygun olmasını sağlayabiliyor. Kısacası, bu özellikler şirket ağına mevcut olan ve aksi halde kolayca suistimal edilebilecek zayıflıklara karşı koruma sağlamaya yardımcı oluyor.
- Comodo Cihaz Yöneticisi (ITSM) hem mobil, hem de masaüstü platformlarda cihaz ve veri güvenliğinin takibini ve yapılması gereken işlemleri tek bir konsoldan yönetme imkanı sunarak bu tehdidi ortadan kaldırıyor. COMODO'nun Uç Nokta Koruma teknolojisi ile desteklenen ITSM (IT and Security Manager) ile firma IT departmanları, buluttan ya da kendi yönetim sunucularından hesaplarına erişerek işlemleri yönetebiliyorlar. Comodo ITSM ile ilgili daha fazla bilgi için; <https://enterprise.comodo.com/itsm>