Dost Acı Söyler…

written by Mert SARICA | 16 February 2010

Yaklaşık 1 hafta önce Netsec e-posta listesine kayıtlı bir üye Symantec DLP ürününde, admin yetkisi ile servislerin kapatılabildiğini gösteren bir video adresi paylaştı ve tartışmalar başladı. Öncelikle bu üyenin başka bir üreticinin (Websense) dağıtıcısı olması nedeniyle bu video adresini paylaşması eleştirilerin ilk hedefi oldu. Daha sonra bu durumun windows'un bir zafiyeti olduğunu söyleyenler oldu, videonun Symantec'i karalama amacıyla bu üye tarafından çekildiğini ve yayınlandığını söyleyenler oldu, system yetkisine sahip kullanıcı lokalde çalışan her programı zaten kapatılabilir diyenler oldu ve tartışmalar böyle sürüp gitti.

Konuya etik açıdan bakılacak olursa bu sektörde yer alan bireyler olarak bilişim güvenliğine önem veriyor, beyaz şapkamız ile iş yapıyor ve her kim olursa olsun, X üreticisinin veya Y üreticisinin müşteriside olsa amacımız masum insanların art niyetli kişilerce istismar edilmesini engellemek, üreticileri güvenli ürünler geliştirmeye teşvik etmek ise bu veya benzer videoları yayınlamadan önce biraz olsun bu durumun ortaya çıkartacağı sorunları ve madur edeceği insanlarıda düşünmek zorundayız. X ürününde bir güvenlik açığı var ise bunu bildirmek ile bu güvenlik açığını istismar eden aracı programlamak ve yayınlamak arasında büyük fark olduğunu düşünüyorum bu nedenle bende çoğu zaman yayınladığım videolarda buna özen gösteriyor, üreticiyi zor durumda bırakmadan insanları bilgilendirmeye çalışıyorum. Benim düşünceme göre hem responsible disclosure adına hem de üreticiler arasındaki gayri resmi centilmenlik anlaşmaları kapsamında bu videonun genel ile paylaşılmadan önce Symantec yetkilileri ile paylaşılmalıydı.

Konuya müşteri/potansiyel müşteri açısından bakılacak olursa eminimki hiçbir kurum, kritik bilgilerinin dışarıya sızdırılmaması için satın aldığı bir ürünün basit bir şekilde devre dışı bırakılmasını istemez. Tartışma yaratan video ile Symantec DLP ürününün rakipleri karşısında process/servis güvenliği açısından geride kaldığı inkar edilemez bir gerçek. Her ne kadar servisleri kapatmak için admin yetkisine ihtiyaç duyulsada örneğin DLP agent'ının üzerinde çalıştığı işletim sistemindeki yamalarda bir eksiklik veya system yetkisi ile çalışan bir yazılımdaki bir zafiyetin istismar edilmesi sonrasında işletim sistemi üzerinde system yetkisi kolayca elde edilebileceği için bu tür çözümlerin kolay bir şekilde devre dışı bırakılmasının pek kabul

edilebilir olduğunu düşünmüyorum. Eğer aksi durum söz konusu olsaydı eminimki ne rakipler ne de antivirus yazılımlarında servislerin/processlerin kolayca kapatılmaması için ek kontroller uygulanmaz ve önlemler alınmazdı.

Tartışmaları ve yorumları bir kenara bırakacak olursak, geçtiğimiz akşam can sıkıntısından Symantec DLP ürünü ile birlikte gelen yönetici kılavuzunu okuyordum ve DLP yönetim araçlarından biri olan process_shutdown programı ile ilgili bölüm dikkatimi çekti. Bu program ile DLP servislerini kapatabiliyorsunuz ancak bunun için DLP agent'ının kullandığı doğru şifreyi bilmeniz gerekiyor. Malum her zamanki can sıkıntısı ve merak ile process_shutdown yazılımını assembly seviyesinde incelemeye başladım ve doğru şifre girmeden servisi kapatabilmenin yollarını aramaya koyuldum ve çok geçmeden bunu başarabildim.

Son söz olarak Symantec DLP çözümünün servis/process güvenliği konusunda iyileştirmeye açık olduğu hem diğer video ile hem de yaptığım bu ufak inceleme ile ortaya çıkıyor. Umarım Symantec en kısa süre içerisinde ürün üzerinde gerekli iyileştirmeleri yaparak bu ürünü servis/process güvenliği konusunda rakipleri ile aynı seviyeye getirir ve bu tartışmalar son bulur.

Not: POC olarak genel izleyici kitlesi için teknik detay içermeyen ve Symantec yetkilileri için teknik detay içeren iki farklı video çektim. Symantec yetkileri ile geçtiğimiz Cuma günü videoyu paylaştım. Genel izleyici kitlesi için hazırlanan video aşağıdadır, iyi seyirler…