TEMEL BİLGİ GÜVENLİĞİ-7

Rootkit

Rootkit bilgisayar üzerinde çalışan programları gizleyen bir yazılım parçasıdır. Bu yüzden zararlı yazılımlar genellikle rootkit'leri yükleyerek bilgisayar üzerindeki faaliyetlerini gizlemeyi amaçlarlar. Bilgisayar ve ağlara yönetici düzeyinde erişim hakkı elde edip, tüm sistemi kontrol edebilecek düzeye gelebilirler.

Rootkitler tek başlarına tehlikeli olmayabilir. Ancak beraberlerinde tehlikeli bir virüs/zararlı yazılım çeşidi ile birlikte yüklendiklerinde ciddi tehlike teşkil ederler. Rootkit keylogger zararlı yazılımlarını, parola çözücü programları saklayarak içerdikleri/topladıkları hassas bilgileri internet aracılığı ile saldırganlara gönderilmesi amacıyla kullanılabilirler.

Rootkitleri antivirüs programlarının tespit etmesi güç olabilmektedir. Bu yüzden endpoint güvenlik ürünlerinde rootkitlerin tespiti ve bilgisayardan kaldırılabilmesi için özel geliştirmeler yapılmıştır. Buna rağmen bazı rootkit zararlı yazılımlarının tespiti ve kaldırılabilmesi için daha kapsamlı ürünler ve stratejiler gerekebilmektedir.

Fake Antivirüs Malware (Sahte Antivirüs Zararlı Yazılımları)

Sahte Antivirüs zararlı yazılımları, bilgisayar kullanıcılarını genellikle sahte virüs tehdidi algılandı uyarısıyla (pop-up mesajı) karşılayarak zararlı yazılımın, virüs temizlemek yada taramak amacıyla indirilmesine teşvik ederler. Bu tip uyarılar genellikle zararlı web sayfalarında görülür ve online virüs tarama dokümanı görüntülerler.

Siber suçlular ise bu yöntemi kullanıcıları zararlı içerik sağlayan sitelere çekerek ya da yasal siteleri ele geçirerek, spam mesajlar göndermek için kullanırlar. Bu tip yazılımların en popüler arama sitelerinde kullanıcıların karşılarına çıktıları görülmektedir.

Sahte antivirüs yazılımları son dönemlerde mobil telefonlar, tabletler de dahil olmak üzere tüm internet erişimli cihazlar için tehlike oluşturmaktadır. Mobil uygulamalara pop-up mesajları olarak günlük hayatta sıklıkla sayısız kullanıcının karşısına çıkabilmektedir. Saldırgan gruplar için finansal karlılık açısından tercih edilen bir yöntem olmaya başlamıştır.

Bu tip yöntemlerle zararlı yazılım bulaşmasının önlenmesi amacı ile yasal antivirüs programları kullanılmalıdır. Bir başka korunma yöntemi ise bu tip tehditlere karşı bilinçli olunmalı ve şüpheli olabilecek linklerden kaçınılmalıdır.

Exploit

Exploit, bilgisayar ve sistem üzerindeki açıklıklardan ya da hatalardan faydalanarak sistemlere sızma amacı taşıyan programlardır. Sistemlere erişim yöntemlerine göre exploitlerin çeşitleri mevcuttur:

- Remote Exploit (Ağ üzerinden sistemle etkileşimde bulunurlar.)
- Local Exploit (Genelde sistemdeki yetkili kullanıcı özelliklerini kullanmak amacıyla oluşturulurlar)
- Client Side Exploit (Sistemle etkileşimde bulunduktan sonra bir kullanıcı tarafından tetiklenerek aktif olurlar)

Saldırganlar için exploitlerin en önemli avantajı sisteme sızarak “yetkili profil” oluşturabilmelidir. Exploitler saldırganlar tarafından açıklıklardan faydalanarak özel amaçlar için kullanılmak üzere tasarlanırlar. Yama yönetimi exploitlerden korunmak için oldukça önemlidir. Spesifik bir açıklık için yama güncellemesi yapıldığında exploitler etkisiz hale gelmektedir.

Zero-day exploit ise açıklık bilinirliği sağlanmadan önce gerçekleştirilen saldırılara verilen isimdir. Üretici/tedarikçi şirket açıklığı yayınlamadan önce zero day exploit saldırıları gerçekleştirilmiş olur. Öyle ki açıklık ilk defa saldırganlar tarafından tespit ediliyor olabilir.

Tüm işletim sistemleri ve uygulamalar exploitlerden etkilenmeye açıktır. Bu nedenle önlem için antivirüs ve endpoint güvenlik yazılımları kullanılmalı ve yama yönetimi gerçekleştiriliyor olmalıdır.