Self Defence

written by Mert SARICA | 19 March 2010

Genelde uç noktada güvenli bir işlemi gerçekleştirmek veya kullanıcının güvenliğini sağlamak amacıyla tasarlanmış programlar ile ilgili dokümanlar okuduğumda veya inceleme şansı bulduğumda merakımı cezbeden ilk konu programın kendi güvenliğini sağlamada ne kadar başarılı olduğu oluyor.

Geçtiğimiz haftalarda Check Point Endpoint Security programına ait bir ajanı (agent) inceleme fırsatı yakaladım. Kısaca Checkpoint EPS programının sahip olduğu bazı güzel özellikleri sıralamak gerekirse;

- Güvenlik duvarı
- Anti-virüs/Anti-spyware
- Güvenli VPN
- Web ataklarına karşı koruma
- Disk şifreleme
- Ağ erişim kontrolü (NAC)

Var olan ve geri kalan diğer özellikler ile ilgili bilgi almak isterseniz Checkpoint'in web sayfasını ziyaret edebilirsiniz.

Öncelikle belirtmem gerekir ki bu ve benzer programları yönetici yetkisi olmadan kapatmak veya kaldırmak pek mümkün olmuyor ancak tahminde edebileceğiniz üzere kimi zaman bu ve benzer programların kullanıcının yönetici yetkisine sahip olduğu işletim sistemi üzerinde çalışması gerekebiliyor bu nedenle son kullanıcının güvenliğini emanet ettiğiniz bu marifetli programlardan kendisini tehditlere karşı korumasına önem vermesini, kolay bir şekilde devre dışı bırakılmamasını veya işletim sisteminden kaldırılmamasını bekliyorsunuz.

Yine bir boş vaktimde sadece tek bir test senaryosu üzerinden gitmek için kollarımı sıvadım ve program ekle/kaldırdan Checkpoint EPS programını yönetici yetkisi ile işletim sisteminden kaldırmaya çalıştım ve bir şifre ekranı ile karşılaştım. Her zamanki gibi acaba debugger ile assembly seviyesinde kaldırma işlemi ile ilişkili programlarda bazı değişiklikler yapsam, hatalı şifre ile programı kaldırabilir miyim sorusuna yanıt ararken kısa süre içerisinde cevabı buldum, evet.

Programı kaldırmaya çalıştığımda kaldırma işlemi ile ilişkili programlar her

seferinde yeni baştan yaratıldığı için disk üzerindeki bu programları değiştirmemin bir işe yaramayacağını anlamam pek uzun sürmedi. Ne yapmalı ne yapmalı derken disk üzerinde modifikasyon olmuyor ise bellekte (memory) olmalı diyerek işe koyuldum ve python ile ufak bir program hazırladım ve başarıyla amacıma ulaştım.

Sonuç olarak art niyetli kişilerin/programların amacına ulaşmalarını zorlaştırma adına Checkpoint'in en azından anti-debug tekniklerine (Kobil firması gibi) programlarında yer vermesi gerektiğini, uç nokta güvenliğine önem veren kurumlara ise her ne program kullanılırsa kullanılsın, her ne önlem alınırsa alınsın kullanıcılara yönetici yetkisi verilmeden önce son bir defa daha düşünülmesi gerektiğini hatırlatmak istiyorum.

Bildiğiniz üzere yazılarımda hem üreticilerin hemde müşterilerin mutsuz olmamaları adına çok fazla teknik detay paylaşmıyor sadece tespit ettiğim sorunu kısaca özetleyen bir video yayınlıyorum, bu konu ile ilgili video aşağıdadır. Bir sonraki yazıda görüşmek dileğiyle herkese keyifli seyirler ve iyi haftasonları dilerim.