Sandboxing

Wikipedia tarafından tanımlandığı gibi, "bilgisayar güvenliği alanında bir kum havuzu, çalışan programları ayırmak için kullanılan bir güvenlik mekanizmasıdır. Genellikle test edilmemiş kodları, doğrulanmamış üçüncü taraflardan gelen güvensiz programları, güvensiz kullanıcıları ve güvensiz web sitelerini çalıştırmak için kullanılır." Bu kavram, malware analizinde de uygulanır: Amacımız, bilinmeyen ve güvenilmeyen bir uygulamayı veya dosyayı izole bir ortamda çalıştırmak ve ne yaptığı hakkında bilgi edinmektir. Malware sandboxing, dinamik analiz yaklaşımının pratik bir uygulamasıdır: ikili dosyayı statik olarak analiz etmek yerine, gerçek zamanlı olarak çalıştırılır ve izlenir. Bu yaklaşımın elbette avantajları ve dezavantajları vardır, ancak kötü amaçlı yazılımın ağ davranışı gibi daha fazla ayrıntı elde etmek için değerli bir tekniktir. Bu nedenle kötü amaçlı yazılımı incelemek için hem statik hem de dinamik analiz yapmak, daha derin bir anlayış kazanmak için iyi bir uygulamadır. Basit bir şekilde, Cuckoo, sandbox kötü amaçlı yazılım analizi yapmanıza olanak tanıyan bir araçtır.

Sandbox Kullanmak

Cuckoo'yu kurmadan, yapılandırmadan ve kullanmadan önce, ne elde etmek istediğinizi ve nasıl elde etmek istediğinizi düşünmek için biraz zaman ayırmalısınız.

Kendinize sormanız gereken bazı sorular:

1. Hangi tür dosyaları analiz etmek istiyorum?
2. İşlemek istediğim analiz hacmi nedir?
3. Analizimi çalıştırmak için hangi platformu kullanmak istiyorum?
4. Dosya hakkında hangi tür bilgilere ihtiyacım var?

İzole bir ortamın oluşturulması (örneğin sanal bir makine) muhtemelen bir sandbox dağıtımının en kritik ve önemli kısmıdır: Dikkatlice ve uygun bir planlama ile yapılmalıdır.

Seçtiğiniz sanallaştırma ürününe başlamadan önce zaten kullanmak istediğiniz bir tasarım planınız olmalıdır. Bu tasarım planı aşağıdakileri tanımlamalıdır:

1. Hangi işletim sistemi, dil ve yama seviyesini kullanacaksınız.
2. Hangi yazılımı yüklemeli ve hangi sürümleri kullanmalısınız (özellikle saldırıları analiz ederken önemlidir).

Otomatik malware analizi belirleyici olmayabilir ve başarısı trilyonlarca faktöre bağlı olabilir: Kötü amaçlı yazılımı bir sanallaştırılmış sistemde yerel bir sistem gibi çalıştırmaya çalışıyorsunuz ve bu başarı her zaman garanti olmayabilir. Hedefiniz, ihtiyacınız olan tüm gereksinimleri karşılayabilen bir sistem oluşturmak ve mümkün olduğunca gerçekçi yapmaya çalışmaktır.

Örneğin, normal kullanımın kasıtlı izlerini bırakmayı düşünebilirsiniz, tarayıcı geçmişi, çerezler, belgeler, resimler vb. Malware'ın bu tür dosyalarla çalışmasını, bunları manipüle etmesini veya çalmasını tasarladıysa, bunu fark edebilirsiniz.

Sanallaştırılmış işletim sistemleri genellikle kendileriyle birlikte birçok iz taşırlar, bu da onları çok kolay tespit edilebilir hale getirir. Bu sorunu abartmamalısınız, ancak bu konuda dikkatli olmak ve mümkün olduğunca fazla sanallaştırma izini gizlemeye çalışmak isteyebilirsiniz. Sanallaştırma algılama teknikleri ve karşı önlemler hakkında internet üzerinde çok fazla literatür bulunmaktadır.

Sistem tasarımınızı ve hazırlığınızı tamamladıktan sonra, sistem prototipini oluşturmaya ve dağıtmaya devam edebilirsiniz. Her zaman bazı şeyleri değiştirme veya hafifletme fırsatınız olacak, ancak unutmayın ki başlangıçta iyi planlama her zaman uzun vadede daha az sorun anlamına gelir.