Başlangıç

Bu, Cuckoo Sandbox'a giriş bölümüdür. Temel kötü amaçlı yazılım analizi kavramlarını, Cuckoo'nun ne olduğunu ve kötü amaçlı yazılım analizine nasıl uydurulabileceğini açıklar.

- Sandboxing
  - Sandbox Kullanmak
- Cuckoo Nedir?
  - Tarihçesi
  - Kullanım Senaryoları
  - Mimarisi
  - Lisans

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.

Cuckoo Nedir?

Cuckoo, açık kaynaklı otomatik kötü amaçlı yazılım analiz sistemi biridir. Bu, dosyaları otomatik olarak çalıştırmak ve analiz etmek ve izole bir işletim sistemi içinde çalışırken kötü amaçlı yazılımın ne yaptığını anlatan kapsamlı analiz sonuçları toplamak için kullanılır. Aşağıdaki türde sonuçları alabilir: - Kötü amaçlı yazılım tarafından oluşturulan tüm işlemler tarafından gerçekleştirilen çağrı izleri. - Kötü amaçlı yazılımın çalıştırılması sırasında oluşturulan, silinen ve indirilen dosyalar. - Kötü amaçlı yazılım işlemlerinin bellek dökümleri. - PCAP biçiminde ağ trafiği izi. - Kötü amaçlı yazılımın yürütülmesi sırasında alınan ekran görüntüleri. - Makinelerin tam bellek dökümleri.

Tarihçesi

Cuckoo Sandbox, 2010 yılında The Honeynet Project bünyesinde Google Summer of Code projesi olarak başladı. Başlangıçta Claudio "nex" Guarnieri tarafından tasarlandı ve geliştirildi ve hala proje lideri ve çekirdek geliştirici olarak görev yapmaktadır.

2010 yazında başlayan ilk çalışmanın ardından, ilk beta sürümü 5 Şubat 2011'de yayımlandı ve Cuckoo ilk kez kamuoyuna duyuruldu ve dağıtıldı.

Mart 2011'de, Cuckoo, The Honeynet Project ile birlikte Google Summer of Code 2011'de desteklenen bir proje olarak yeniden seçildi ve Dario Fernandes proje ekibine katılarak işlevselliğini genişletti.

2 Kasım 2011'de Cuckoo, ilk gerçek kararlı sürüm olarak 0.2 sürümünü kamuoyuna duyurdu. Kasım 2011'in sonlarında Alessandro "jekil" Tanasi ekibe katılarak Cuckoo'nun işleme ve raporlama işlevselliğini genişletti.

Aralık 2011'de Cuckoo v0.3 sürümü yayımlandı ve hızla Şubat'ın başlarında 0.3.2 sürümüne ulaştı.

Mart 2012'de Cuckoo Sandbox, Rapid7 tarafından düzenlenen Magnificent7 programının ilk turunu kazandı.

2012 Yazı sırasında Jurriaan "skier" Bremer geliştirme ekibine katıldı ve Windows analiz bileşenini ciddi şekilde yeniden düzenledi ve analiz kalitesini önemli ölçüde artırdı.

24 Temmuz 2012'de Cuckoo Sandbox 0.4 sürümü yayımlandı.

20 Aralık 2012'de Cuckoo Sandbox 0.5 "To The End Of The World" sürümü yayımlandı.

1 Ağustos 2013'te Claudio "nex" Guarnieri, Jurriaan "skier" Bremer ve Mark "rep" Schloesser, Black Hat Las Vegas'ta "Mo' Malware Mo' Problems - Cuckoo Sandbox to the rescue" başlıklı bir sunum yaptılar.

9 Ocak 2014'te Cuckoo Sandbox 1.0 sürümü yayımlandı.

Mart 2014'te Cuckoo Vakfı, Cuckoo Sandbox ve çevresindeki projeler ve girişimlerin büyümesine adanmış kar amacı gütmeyen bir kuruluş olarak kuruldu.

7 Nisan 2014'te Cuckoo Sandbox 1.1 sürümü yayımlandı.

7 Ekim 2014'te, Cuckoo Sandbox 1.1.1 sürümü, Robert Michel tarafından açıklanan Kritik Bir Güvenlik Açığından sonra yayımlandı.

4 Mart 2015'te Cuckoo Sandbox 1.2, Cuckoo'nun kullanılabilirliği konusunda bir dizi iyileştirmeyi içeren bir sürüm olarak yayımlandı.

2015 yazında, Cuckoo Sandbox, The Honeynet Project bünyesinde bir Google Summer of Code projesi olarak Mac OS X kötü amaçlı yazılım analizi geliştirmeye başladı. Dmitry Rodionov, projeyi kalifiye oldu ve Mac OS X için çalışan bir analiz programı geliştirdi.

21 Şubat 2016'da 2.0 Sürüm Adayı 1 yayımlandı. Bu sürüm, Cuckoo Sandbox'ı günlük kullanım için daha iyi bir proje yapmak için iki yıla yakın bir sürenin birleşimini içermektedir.

Kullanım Senaryoları

Cuckoo, son derece modüler tasarımı sayesinde hem bağımsız bir uygulama olarak hem de daha büyük çerçevelere entegre edilmek üzere tasarlanmıştır.

Cuckoo, şunları analiz etmek için kullanılabilir:

- Genel Windows uygulamaları
- DLL dosyaları
- PDF belgeleri
- Microsoft Office belgeleri
- URL'ler ve HTML dosyaları
- PHP betikleri
- CPL dosyaları
- Görsel Temel (VB) betikleri
- ZIP dosyaları
- Java JAR
- Python dosyaları
- Neredeyse her şey

Modüler yapısı ve güçlü komut dosyası yetenekleri sayesinde, Cuckoo ile ne elde edebileceğiniz konusunda sınır yoktur.

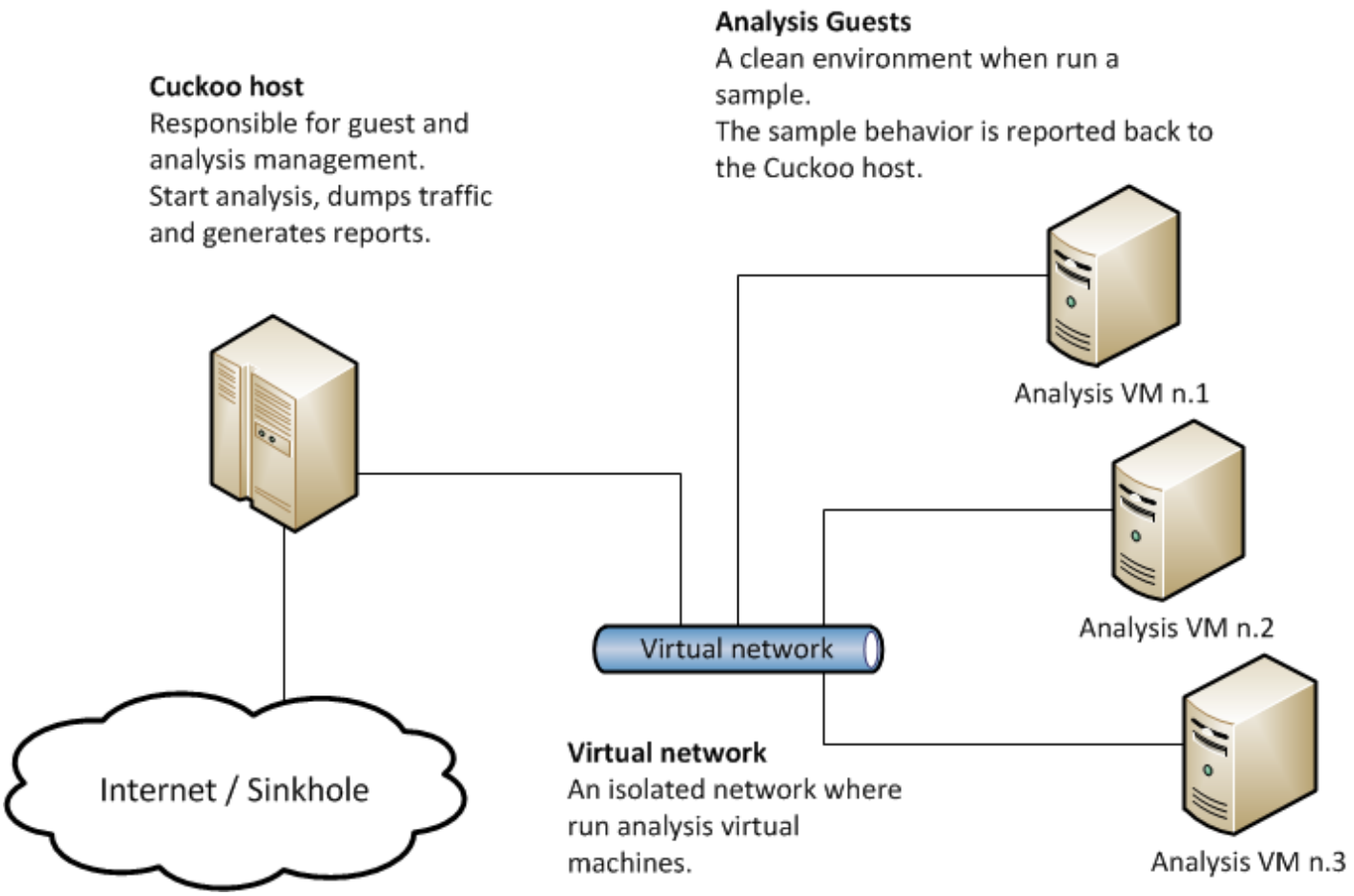
Mimarisi

Cuckoo Sandbox, örnek yürütme ve analizi işleyen merkezi bir yönetim yazılımından oluşur.

Her analiz, taze ve izole bir sanal veya fiziksel makinede başlatılır. Cuckoo'nun altyapısının başlıca bileşenleri, Bir Ana Makine (yönetim yazılımı) ve bir dizi Konuk Makine (analiz için sanal veya fiziksel makineler) içerir.

Ana Makine, tüm analiz sürecini yöneten sandbox'ın temel bileşenini çalıştırırken, Konuklar, kötü amaçlı yazılım örneklerinin gerçekten güvenli bir şekilde yürütüldüğü ve analiz edildiği izole ortamlardır.

Aşağıdaki resim, Cuckoo'nun temel mimarisini açıklar:



Lisans

Cuckoo Sandbox lisansı, Cuckoo ile birlikte gelir ve "docs" klasörü içindeki "LICENSE" dosyasında bulunur.