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
- Kullanım Senaryoları
- Mimarisi
- Lisans

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.

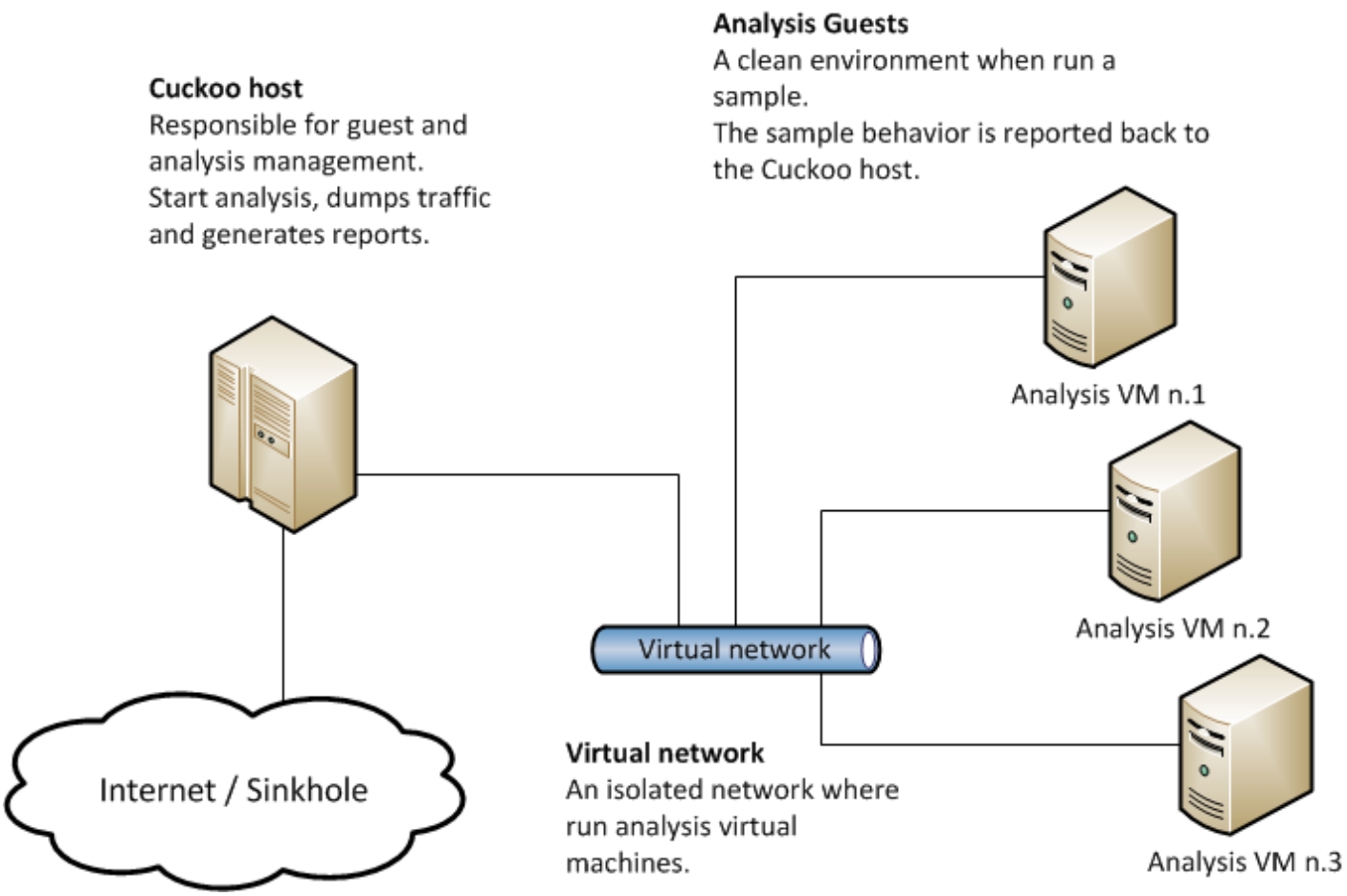
Mimarisi

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.