Analiz Paketleri

Analiz paketleri, Cuckoo Sandbox'ın temel bir bileşenidir. Bunlar, konuk makinelerde yürütüldüğünde Cuckoo'nun analizör bileşeninin analizi nasıl yürütmesi gerektiğini açıklayan yapılandırılmış Python sınıflarından oluşur.

Cuckoo, kullanabileceğiniz bazı varsayılan analiz paketleri sağlar, ancak kendi paketlerinizi oluşturabilir veya mevcut olanları değiştirebilirsiniz. Bunları `analyzer/windows/modules/packages/` dizininde bulabilirsiniz.

Analiz paketlerine Analiz bölümünde açıklandığı gibi `key1=value1,key2=value2` şeklinde bazı seçenekleri belirtebilirsiniz. Mevcut analiz paketleri zaten etkinleştirilebilecek bazı varsayılan seçenekleri içerir.

Aşağıda, açıkça belirtilmedikçe tüm analiz paketleri için çalışan seçeneklerin bir listesi bulunmaktadır:

- free [yes/no]: etkinleştirildiyse, davranışsal günlükler oluşturulmaz ve kötü amaçlı yazılım serbestçe çalıştırılır.
- procmemdump [yes/no]: etkinleştirildiyse, tüm aktif olarak izlenen süreçlerin bellek dökümlerini alır.
- human 0: devre dışı bırakıldığında, insan benzeri etkileşim (örneğin, fare hareketleri) etkinleştirilmez.

Aşağıda, alfabetik sırayla mevcut paketlerin bir listesi bulunmaktadır:

- applet: Java applet'leri analiz etmek için kullanılır. Seçenekler:
  - class: Yürütülecek sınıfın adını belirtin. Bu seçenek, doğru bir yürütme için zorunludur.
- bin: Genel binary veri, örneğin shellcode'ları analiz etmek için kullanılır.
- cpl: Control Panel Applet'lerini analiz etmek için kullanılır.
- dll: Dinamik Bağlantılı Kütüphaneleri çalıştırmak ve analiz etmek için kullanılır. Seçenekler:
  - function: Yürütülecek işlevi belirtin. Hiçbiri belirtilmezse, Cuckoo DllMain'ı çalıştırmaya çalışacaktır.
  - arguments: DLL'ye komut satırından iletilmesi için argümanları belirtin.
  - loader: Belirli kötü amaçlı yazılımların olası anti-sandbox hilelerini kandırmak için kullanılabilen rundll32.exe'nin yerine kullanılacak bir işlem adını belirtin.
- doc: Microsoft Word belgelerini çalıştırmak ve analiz etmek için kullanılır.
- exe: Genel Windows yürütülebilir dosyalarını analiz etmek için kullanılan varsayılan analiz paketi. Seçenekler:
  - arguments: Gönderilen kötü amaçlı yazılımın başlangıç sürecine iletilmek üzere herhangi bir komut satırı argümanını belirtin.

- generic: cmd.exe aracılığıyla genel örnekleri çalıştırmak ve analiz etmek için kullanılır.
- ie: Verilen URL veya HTML dosyasını açarken Internet Explorer'ın davranışını analiz etmek için kullanılır.
- jar: Java JAR konteynerlerini analiz etmek için kullanılır. Seçenekler:
  - class: Yürütülecek sınıfın yolunu belirtin. Hiçbiri belirtilmezse, Cuckoo Jar'ın MANIFEST dosyasında belirtilen ana işlemleri çalıştırmaya çalışacaktır.
- js: Javascript dosyalarını çalıştırmak ve analiz etmek için kullanılır (örneğin, e-posta eklerinde bulunanlar).
- hta: HTML Uygulama dosyalarını çalıştırmak ve analiz etmek için kullanılır.
- msi: MSI Windows yükleyiciyi çalıştırmak ve analiz etmek için kullanılır.
- pdf: PDF belgelerini çalıştırmak ve analiz etmek için kullanılır.
- ppt: Microsoft PowerPoint belgelerini çalıştırmak ve analiz etmek için kullanılır.
- ps1: PowerShell betiklerini çalıştırmak ve analiz etmek için kullanılır.
- python: Python betiklerini çalıştırmak ve analiz etmek için kullanılır.
- vbs: VBScript dosyalarını çalıştırmak ve analiz etmek için kullanılır.
- wsf: Windows Script Host dosyalarını çalıştırmak ve analiz etmek için kullanılır.
- xls: Microsoft Excel belgelerini çalıştırmak ve analiz etmek için kullanılır.
- zip: Zip arşivlerini çalıştırmak ve analiz etmek için kullanılır. Seçenekler:
  - file: Arşivde bulunan dosyanın adını belirtin. Hiçbiri belirtilmezse, Cuckoo örnek.exe'yi çalıştırmaya çalışacaktır.
  - arguments: Gönderilen kötü amaçlı yazılımın başlangıç sürecine iletilmek üzere herhangi bir komut satırı argümanını belirtin.
  - password: Arşivin şifresini belirtin. Hiçbiri belirtilmezse, Cuckoo arşivi şifresiz çıkarmaya veya "infected" şifresini kullanmaya çalışacaktır.

  Zaten bildiğiniz gibi, analiz paketini seçmek için gönderim sırasında (Analiz'e bakın) aşağıdaki gibi adını belirterek kullanabilirsiniz:

```
$ cuckoo submit --package <package name> /path/to/malware
```

Hiçbiri belirtilmezse, Cuckoo dosya türünü algılamaya çalışacak ve buna göre doğru analiz paketini seçecektir. Dosya türü varsayılan olarak desteklenmiyorsa, analiz durdurulacaktır, bu nedenle mümkünse paket adını belirtmenizi öneririz.

Örneğin, kötü amaçlı yazılımı başlatmak ve bazı seçenekleri belirtmek için şu adımları izleyebilirsiniz:

```
$ cuckoo submit --package dll --options
function=FunctionName,loader=explorer.exe /path/to/malware.dll
```

Analiz Sonuçları

Bir analiz tamamlandığında, çeşitli dosyalar özel bir dizine kaydedilir. Tüm analizler, analiz görevini veritabanında temsil eden artan sayısal ID'ye göre adlandırılmış bir alt dizin içinde `$CWD/storage/analyses/` altında saklanır.

Aşağıda bir analiz dizin yapısının örneği bulunmaktadır:

```
.
|-- analysis.log
|-- binary
|-- dump.pcap
|-- memory.dmp
|-- files
|   |-- 1234567890_dropped.exe
|-- logs
|   |-- 1232.bson
|   |-- 1540.bson
|   `-- 1118.bson
|-- reports
|   |-- report.html
|   |-- report.json
`-- shots
    |-- 0001.jpg
    |-- 0002.jpg
    |-- 0003.jpg
    `-- 0004.jpg
```

analysis.log

Bu, içerideki konuk ortamında gerçekleşen analiz yürütmenin izini içeren analizör tarafından oluşturulan bir günlük dosyasıdır. Bu, süreçlerin, dosyaların oluşturulmasını ve yürütme sırasında meydana gelen olası hataları raporlayacaktır.

dump.pcap

Bu, tcpdump veya diğer ilgili herhangi bir ağ dinleyicisi tarafından oluşturulan ağ dökümüdür.

dump_sorted.pcap

Bu, web arayüzü'nün TCP akışını hızlı bir şekilde aramasına izin veren dump.pcap'in sıralanmış bir versiyonudur.

memory.dmp

Etkinleştirilmiş olmanız durumunda, bu dosya analiz makinesinin tam bellek dökümünü içerir.

files/

Bu dizin, kötü amaçlı yazılımın üzerinde çalıştığı ve Cuckoo'nun dökebildiği tüm dosyaları içerir.

files.json

Bu dosya, mevcut tüm bırakılmış dosyalar için (yani, files/, shots/, vb. içindeki tüm dosyalar) her biri için bir JSON kodlu giriş içerir. Dosya hakkında mevcut olan tüm süreçlerle ilgili meta bilgileri içerir, konukta orijinal dosya yolu vb.

logs/

Bu dizin, Cuckoo'nun süreç izlemesi tarafından oluşturulan tüm raw günlükleri içerir.

reports/

Bu dizin, Konfigürasyon bölümünde açıklandığı gibi Cuckoo tarafından oluşturulan tüm raporları içerir.

shots/

Bu dizin, kötü amaçlı yazılım yürütme sırasında konuğun masaüstünün tüm ekran görüntülerini içerir.

tlsmaster.txt

Bu dosya, analiz sırasında yakalanan TLS Master Secrets'ları içerir. TLS Master Secrets, SSL/TLS trafiğini şifrelemek için kullanılabilir ve bu nedenle HTTPS akışlarını şifrelemek için kullanılır.

Tüm Görevleri ve Örnekleri Temizlemek

Sürüm 2.0.0'de Değişiklik: Bağımsız bir komut dosyası yerine düzgün bir Cuckoo Uygulamasına dönüştürüldü.

Cuckoo 1.2'den bu yana yerleşik bir temizleme özelliği bulunmaktadır. Bu özellik, veritabanındaki görevlerin ve örneklerin tüm ilişkili bilgilerini, sabit diskten, MongoDB'den ve ElasticSearch'ten bırakır. Clean'i çalıştırdıktan sonra bir görev gönderirseniz, `Task #1` ile tekrar başlarsınız.

Temizlemek için aşağıdaki komutu çalıştırın:

```
$ cuckoo clean
```

Özetle, bu komut şunları yapar:

- Analiz sonuçlarını siler.
- Gönderilen binary dosyaları siler.
- Yapılandırılmış veritabanındaki görevlerin ve örneklerin tüm ilişkili bilgilerini siler.
- Yapılandırılmış MongoDB veritabanındaki tüm verileri siler (eğer `$CWD/conf/reporting.conf`'da yapılandırılmış ve etkinse).
- Yapılandırılmış ElasticSearch veritabanındaki tüm verileri siler (eğer `$CWD/conf/reporting.conf`'da yapılandırılmış ve etkinse).

> Bu komutu kullanırsanız, Cuckoo tarafından tüm mevcut depolama alanlarında (dosya sistemi, SQL veritabanı, MongoDB veritabanı ve ElasticSearch veritabanı) depolanan tüm verileri kalıcı olarak sileceksiniz. Bu komutu yalnızca tüm verileri temizleyeceğinizden emin olduğunuzda kullanın.

Revision #1
Created 19 January 2024 11:36:48 by Ertan Sözer
Updated 19 January 2024 11:42:38 by Ertan Sözer