Genel Sorular

- Cuckoo ile URL'leri analiz edebilir miyim?
- Cuckoo ile Volatility'i kullanabilir miyim?
- Cuckoo'yu VMware ESXi ile kullanabilmek için neler gereklidir?

Cuckoo ile URL'leri analiz edebilir miyim?

Sürüm 0.5 ile gelen yeni özellik: Cuckoo'ya URL analizi için yerleşik destek eklendi.

Sürüm 2.0-rc1'de değişiklik: Cuckoo artık sadece tarayıcıyı başlatmakla kalmayacak (örneğin Internet Explorer), aynı zamanda ilginç sonuçlar çıkarmak için etkili bir şekilde enstrüman yapmaya çalışacaktır; bu sonuçlar arasında yürütülen JavaScript, iframe URL'leri gibi veriler bulunur.

URL gönderimi hakkında ek ayrıntılar, bir Analiz Gönderme konusunda belgelenmiştir, ancak özünde şu komutu içerir:

```
cuckoo submit --url http://example.com
```

Cuckoo ile Volatility'i kullanabilir miyim?

Sürüm 0.5 ile yeni eklenen özellik: Cuckoo, analiz sürecinin sonunda oluşturulan isteğe bağlı memory dump destekler. Bu memory dumpları kullanarak Volatility gibi memory forensic analizlerini gerçekleştirebilirsiniz.

Ayrıca, lütfen bunu özellikle teşvik etmediğimizi göz önünde bulundurun: Cuckoo, işlemlerini gerçekleştirmek için bazı rootkit benzeri teknolojiler kullanır, bu nedenle bir forensic analizin sonuçları, sandbox'ın bileşenleri tarafından kirletilebilir.

Cuckoo'yu VMware ESXi ile kullanabilmek için neler gereklidir?

VMware vSphere Hypervisor (veya ESXi) ile çalıştırmak için, Cuckoo, libvirt veya VMware vSphere API için Python SDK olan pyVmomi'ye dayanır. Sanal makineler üzerinde kontrol sağlamak için VMware API'leri kullanılır, ancak bu API'ler yalnızca lisanslı sürümde bulunur. VMware vSphere ücretsiz sürümünde bu API'ler yalnızca okunurdur, bu nedenle Cuckoo ile kullanamazsınız. Minimum gerekli lisans için lütfen VMware web sitesine göz atın.