Auxiliary Modülleri

Yardımcı modüller, her tek analiz sürecine paralel olarak yürütülmesi gereken bazı prosedürleri tanımlar. Tüm yardımcı modüllerin `cuckoo/cuckoo/auxiliary/` dizini altına yerleştirilmesi gerekir, bu şekilde modül `cuckoo.auxiliary` modülü altına düşer.

Bir modülün yapısı aşağıdakine benzerdir:

```
from cuckoo.common.abstracts import Auxiliary

class MyAuxiliary(Auxiliary):

    def start(self):
        # Do something.

    def stop(self):
        # Stop the execution.
```

`start()` fonksiyonu, analiz makinesini başlatmadan önce ve gönderilen kötü amaçlı dosyayı etkili bir şekilde yürütmek üzere başlatılacaktır, `stop()` fonksiyonu analiz sürecinin sonunda, işleme ve raporlama prosedürlerini başlatmadan önce başlatılacaktır.

Örneğin, Cuckoo tarafından varsayılan olarak sağlanan bir yardımcı modül `sniffer.py` olarak adlandırılır ve oluşturulan ağ trafiğini dump etmek için tcpdump'ı çalıştırmaktan sorumludur.

Revision #1
Created 19 January 2024 11:44:21 by Ertan Sözer
Updated 19 January 2024 11:44:54 by Ertan Sözer