Cuckoo Working Directory ve Konfigürasyonu

Yeni sürüm 2.0.0'da yeni bir konsept olan `Cuckoo Working Directory` tanıtıldı. Bu noktadan itibaren, Cuckoo'nun yapılandırılabilir tüm bileşenleri, oluşturulan veriler ve sonuçlar bu dizinde depolanmaktadır. Bu dosyalar arasında şunlar bulunabilir ancak bunlarla sınırlı değildir:

- Yapılandırma
- Cuckoo İmzaları
- Cuckoo Analizörü
- Cuckoo Ajanı
- Yara kuralları
- Cuckoo Depolama (analiz sonuçlarının gittiği yer)
- Ve daha fazlası...

`Cuckoo Working Directory`, Cuckoo'nun önceki yaklaşımına göre birkaç avantaj sunmaktadır. İlerleyen bölümlerde, Cuckoo Çalışma Dizini'nin (CWD) çeşitli günlük engelleri nasıl aştığını inceleyeceğiz.

Eğer Cuckoo kurulumunuzu daha yeni bir sürüme güncellediyseniz, yapılandırmanızın yedeğini almanız, Cuckoo örneğinizi güncellemeniz ve yapılandırmanızı ya geri yüklemeniz ya da tamamen yeniden uygulamanız gereken bir sorunla karşılaşmış olabilirsiniz.

`CWD`'nin tanıtılması ile bu güncelleme kabusu bitmiş oluyor.

Cuckoo'yu ilk kez çalıştırdığınızda, `CWD` kontrolü sizin için otomatik olarak oluşturulur, bu aşağı yukarı şu şekilde gerçekleşir:

```
$ cuckoo -d


     _    _           _       _        _       _
    /\ \  /\_\        /\ \     /\_\     /\ \    /\ \
    / \\ ///     _  / \\     /// _    / \\    / \\
    /\\ \\\__   /\_\/\\   ///  /\_\  /\\ \  /\\ \\
  //\\ \\___\  ///// /\\  ///__/// //\\ \ //\\ \\
  /// \\_\ \__ / ///// \\_\ /\_____// /// \\_\/// \\_\
  ///  \/_/ /// /////  \/_/ /\______/ /// /////// ///
  ///     /// /////     //\\  /// /////// ///
 ///_______ ///__/////_______ /// \\\ ///__/////__///
```

```
/ / /_________\/ / /___\/ // / /_________\/ / /    \ \ \ / / /___\/ // / /___\/ /
\/___________/\/_________/ \/___________/\/_/      \_\_\\/_________/ \/_________/

Cuckoo Sandbox 2.0.0
www.cuckoosandbox.org
Copyright (c) 2010-2017

================================================================================
    Welcome to Cuckoo Sandbox, this appears to be your first run!
    We will now set you up with our default configuration.
    You will be able to modify the configuration to your likings
    by exploring the /home/cuckoo/.cuckoo directory.

    Among other configurable things of most interest is the
    new location for your Cuckoo configuration:
            /home/cuckoo/.cuckoo/conf
================================================================================

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).
```

Bilgi mesajları tarafından belirtildiği gibi, `CWD`'nizi artık varsayılan olarak `~/.cuckoo` şeklinde bulabileceksiniz, yani `/home/cuckoo/.cuckoo`. Bildiğiniz gibi tüm yapılandırma dosyalarını `$CWD/conf` dizininde bulabilirsiniz. Yani, `$CWD/conf/cuckoo.conf`, `$CWD/conf/virtualbox.conf` vb.

Şimdi, `CWD` dizini Cuckoo'nun kendisinin bir parçası olmadığından, yani Git deposunun veya en son sürümlerden birinin bir parçası olmadığından, `CWD`'yi ellemeye gerek kalmadan Cuckoo'yu yükseltebileceksiniz. (Tabii ki, güncellenmiş bir Yapılandırma gerektiren bir güncelleme yüklenirse, yapılandırma dosyalarını kendisi üzerine yazmak yerine Cuckoo kullanıcıyı bununla ilgili olarak yönlendirecektir).

Revision #1
Created 25 December 2023 08:04:46 by Ertan Sözer
Updated 25 December 2023 08:06:12 by Ertan Sözer