tcpdump Kurulumu

Malware'nin yürütülme sırasında gerçekleştirdiği ağ etkinliğini yakalamak ve bu trafiği bir dosyaya dökmek için uygun şekilde yapılandırılmış bir ağ dinleyiciye ihtiyacınız olacaktır.

Varsayılan olarak, Cuckoo, önde gelen açık kaynak çözümü olan tcpdump'ı kullanır.

Ubuntu'da kurulumu yapmak için:

```
$ sudo apt-get install tcpdump apparmor-utils
$ sudo aa-disable /usr/sbin/tcpdump
```

AppArmor profil devre dışı bırakma (aa-disable komutu) yalnızca varsayılan CWD dizinini kullandığınızda gereklidir, aksi takdirde AppArmor gerçek PCAP dosyalarının oluşturulmasını engeller (bkz. tcpdump Permission Denied hatası).

AppArmor devre dışı bırakılmış (örneğin Debian gibi) Linux platformları için tcpdump'u kurmak için aşağıdaki komut yeterlidir:

```
$ sudo apt-get install tcpdump
```

Tcpdump, root ayrıcalıklarını gerektirir, ancak Cuckoo'nun root yetkileriyle çalışmasını istemediğiniz için binary dosyasına belirli Linux yetkileri ayarlamalısınız:

```
$ sudo groupadd pcap
$ sudo usermod -a -G pcap cuckoo
$ sudo chgrp pcap /usr/sbin/tcpdump
$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

Son komutun sonuçlarını şu şekilde doğrulayabilirsiniz:

```
$ getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

Eğer setcap yüklü değilse, aşağıdaki komutla yükleyebilirsiniz:

```
$ sudo apt-get install libcap2-bin
```

Aksi takdirde (tavsiye edilmez), aşağıdaki komutu kullanabilirsiniz:

```
$ sudo chmod +s /usr/sbin/tcpdump
```

Lütfen unutmayın ki setcap yöntemi dahi, potansiyel güvenlik açıkları nedeniyle, sistemin diğer güvenilir olmayan potansiyel kullanıcılarına sahip olduğu durumlarda tamamen güvenli değildir. Cuckoo'yu ayrılmış bir sistemde veya ayrıcalıklı tcpdump yürütmesinin başka şekilde sınırlı olduğu güvenilir bir ortamda çalıştırmanızı tavsiye ederiz.

Revision #2
Created 25 December 2023 07:44:13 by Ertan Sözer
Updated 25 December 2023 07:49:02 by Ertan Sözer