# Que nous apprend cuckoo sur un malware

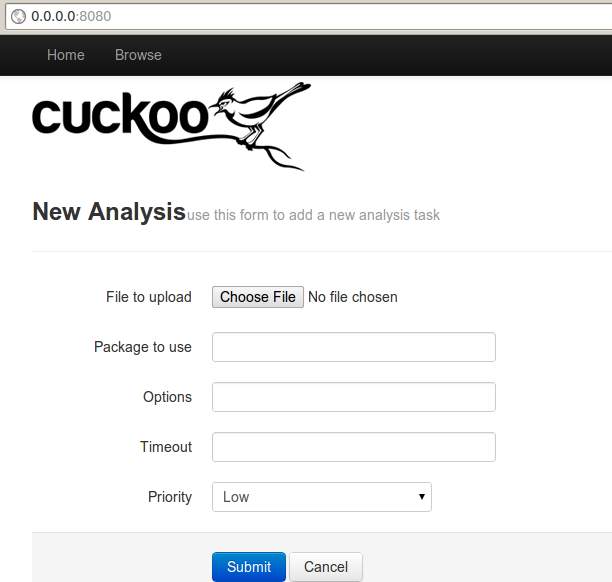
Le lancement du serveur web de cuckoo permettant de soumettre des objets à analyser est exécuté par le fichier /opt/cuckoo/utils/web.py

La première exécution de ce script levait une erreur

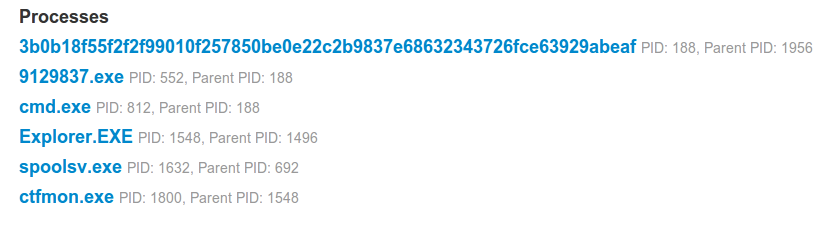
Macintosh HD:Users:Bruno:Desktop:Capture d’écran 2013-03-26 à 19.37.46.png

Erreur résolue en téléchargeant la dernière version de bottle.py (0.11.6) et en la mettant dans le même dossier que web.py

Macintosh HD:Users:Bruno:Desktop:Capture d’écran 2013-03-26 à 19.39.08.png



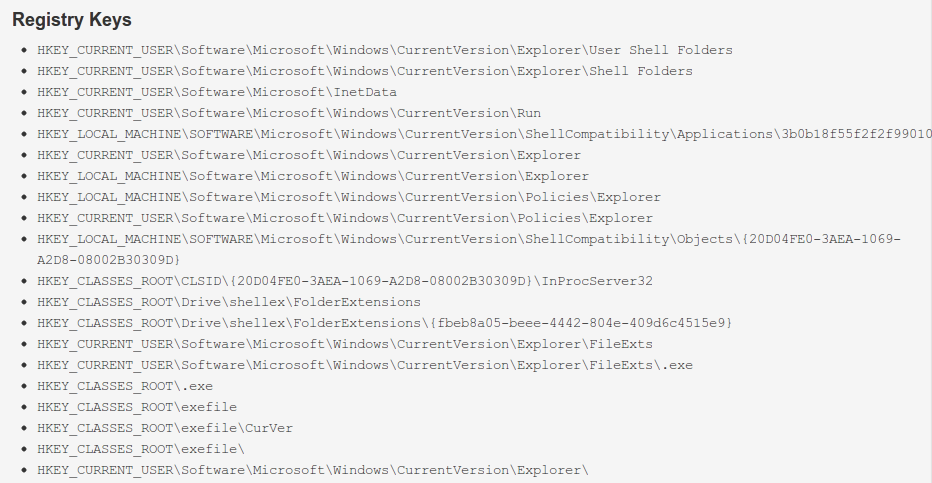
Cuckoo nous rapporte beaucoup de choses intéressantes telles que les processus utilisés par un malware



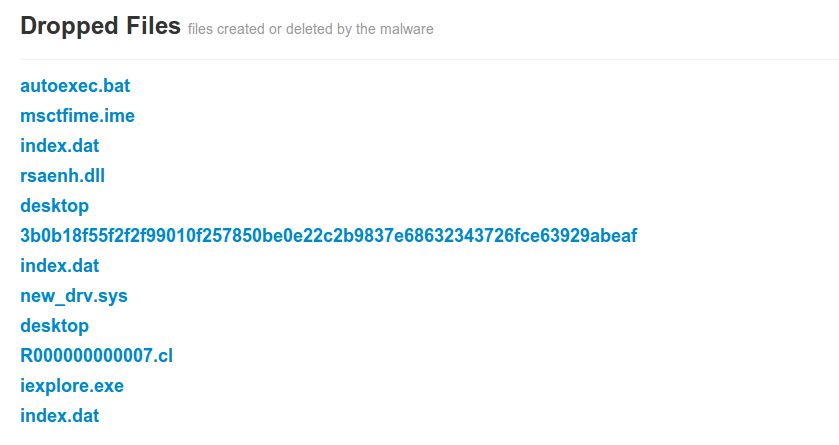
Tous les fichiers visités ou survolés par le malware



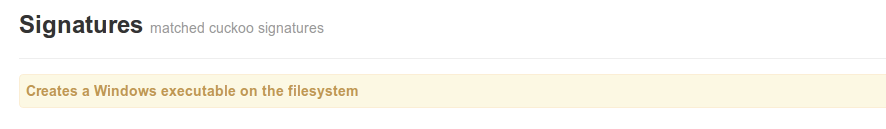
Les clés de registres modifiés ou survolées par ce derniers



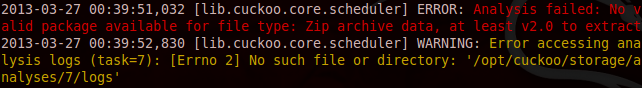
Les fichiers créés, modifier ou supprimer par le malware



Ou encore les signatures du malware comme le fait de créer des exécutables dans le files system qui seront à coup sur des backdoors



Cuckoo ne semble pas encore savoir analyser les zip ou tar ou tar.gz au vue de ce type d’erreurs que j’ai eu pour les 3 zips du set de malware 41190b4f66f511e28c5f33aa9ed05181-snifula



J’ai compris à la suite de cette erreur que le champ package de l’interface web de cuckoo servait à spécifier quel type de fichier nous allions lui donner à analyser tel que dll, bin, zip, doc, exe, ie, jar…

J’ai donc extrait le premier des trois zip (8ae35e87067faf1e9ade47f8002492a2af8810c 102a6c33e0727e7bb4b829f62) pour me rendre compte que celui-ci contenait un fichier .pdf.exe

# Tentative d’analyse avec le package « exe » de cuckoo pour le malware 8ae35e87067faf1e9ade47f8002492a2af8810c 102a6c33e0727e7bb4b829f62)

Ici le rapport nous indique que ce malware à une signature de type **Creates a Windows executable on the filesystem.**

Il crée ou supprime 3 fichiers dont 37679041.pdf.exe



Ce malware semble rechercher s’il est exécuter à l’intérieur d’une machine virtuelle car il parcourt le dossier \Temp\VBoxGuestAdditions\ qui appartient à VirtualBox (ce nom est celui du package nécessaire pour l’activation des pilotes avancées perméttant le drag&drop, l’accélération3D et autres à l’intérieur d’une machine exécuté dans VirtualBox).