2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport de défense n°D005]

SOMMAIRE

I. Description

N° d'attaque subie
Attaque n°5 sur notre serveur

Groupe ayant réalisé l'attaque
Aucune idée

Date de l'attaque
Entre le 19 mars 2014 et le 22 mars 2014

Catégorie d'attaque
Dos par changement de mot de passe

Technique utilisée
Aucune idée, il peut y avoir plusieurs manières :
-bruteforce (impossible, il y a une sécurité mais on ne sait jamais)
-social engeenering
-Tout simplement notre faille qui a été trouvée

CID
Les 3 critères ont été touchés.

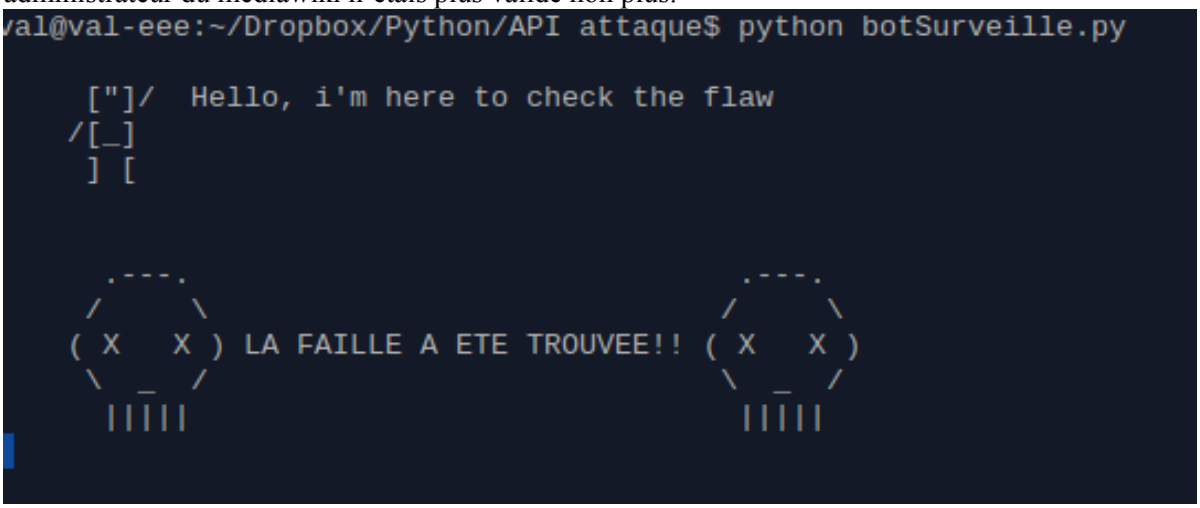
II. Dégâts subit

Description des dégâts

Dos de l'application, vol de mots de passes

Traces / Preuves laissées

Impossibilité de se connecter au compte du bot de notre application, le robot python prévu pour vérifier que la faille n'a pas été trouvée c'est déclenché. De plus, le mot de passe du compte administrateur du mediawiki n'étais plus valide non plus.



III. Contre(s) mesure(s) mise(s) en place

- Changement des mots de passes par des plus complexes à l'aide de script de maintenance de mediawiki.
- Désactivation de la possibilité de changer les mots de passe dans le code source de mediawiki
- Arrêt de simulation de la faille.