2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A002]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 2
Adresse(s) IP cible : 172.24.141.124
Propriétaires du serveur (les 4 noms)
- DEBUF
- KAISER
- DEBRA
- JANATI

Nom de l'attaque
Flush de tous les articles du wiki cible

Date de l'attaque
21/01/2014

Catégorie d'attaque
Attaque par bot python

Technique utilisée
Bot python intelligent threadé utilisant l'API écrite pour le projet de synthèse

Le bot fonctionne de cette manière:
1. Il récupère tous les articles présent sur le wiki cible en utilisant une fonctionnalité de l'API.
2. Il modifie tous les articles par des articles "pierre tombale" ou "tête de mort" (voir screenshots)
3. Il se met en veille un certain temps
4. Il itère les processus 1), 2), 3) et 4) jusqu'à ce que le bot sois arrêté par celui qu'il l'a lancé.

Le bot prend plusieurs options:
- --host => la cible du bot
- -l => le login pour le wiki
- -p => le password du login pour le wiki
- -alfu => le bot vas "Flush" tous les articles (les effacer)
- -alfo => le bot vas flooder le wiki avec plein d'articles aléatoires (En cours de rédaction, non implémenté pour le moment => sois --aflu sois --aflo, pas les deux en même temps)
- --silent => le bot affiche le minimum de texte
- -nt => le nombre de thread à lancer (défaut:1)
- -s => le temps de mise en veille (défaut:60)

Le bot est intelligent car:
1. Il peut se connecter en utilisant un login et un MDP de passe fournit en paramètre
2. Il "flush" (efface) les articles de façon itérative et adapte sa rapidité aux systèmes de défense mis en place: si il est repéré, il va continuer son travail mais de façon plus discrète:
   - il va augmenter le temps entre chaque effacement d'article jusqu'à ce qu'il ne soit plus repéré.
   - il ce "souviens" des articles déjà effacés ce qui fait qu'il ne recommence pas tout au début si jamais il est rejeté par les défenses adverses.

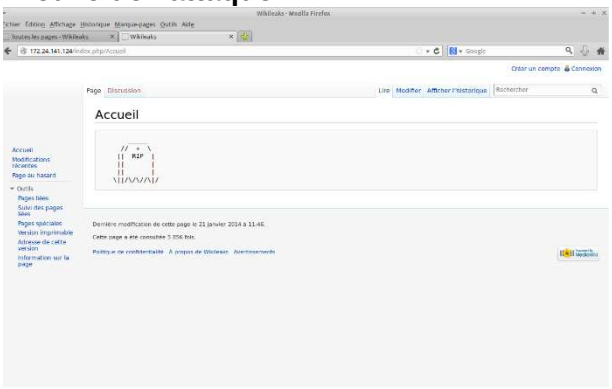
CID
Le bot va toucher la disponibilité dans un premier temps car les articles ne seront plus disponibles. Dans un deuxième temps c'est l'intégrité qui sera touchée: nous savons que les articles peuvent être rétablis via l'historique, or on faisant tourner le bot de façon massive (possibilité de multithread), nous pouvons remplacer les bonnes versions de l'article par ceux du bot (une sorte d'effacement d'historique).

II. Résultat de l'attaque

Description du résultat

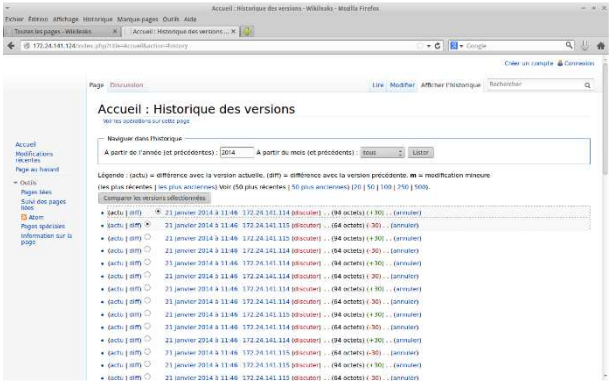
Défiguration totale des articles du wiki, tous remplacés par une "pierre tombale" ou "tête de mort"

Preuve de l'attaque



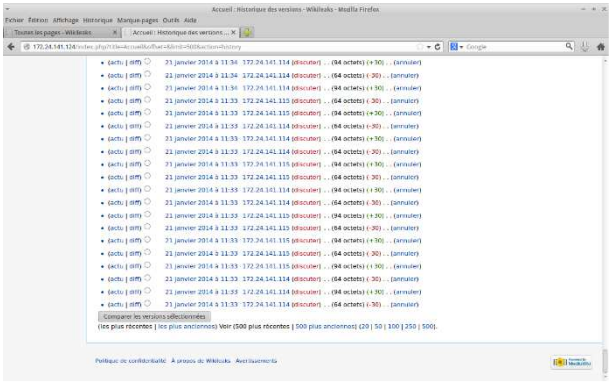
Screen 1

Page d'accueil avec la "pierre tombale"



Screen 2

Historique de la page accueil (début)

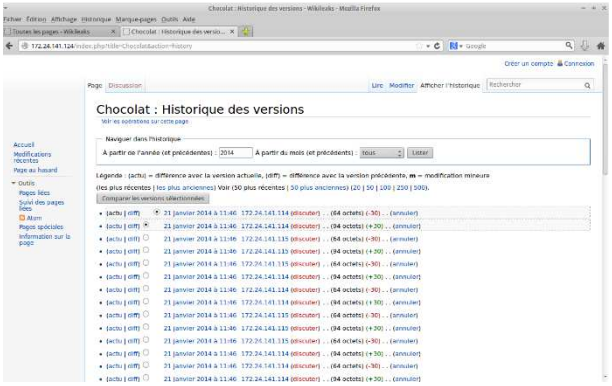


Screen 3

Historique de la page accueil (fin), on peut voir que l'historique s'arrête à 500, le reste a disparu

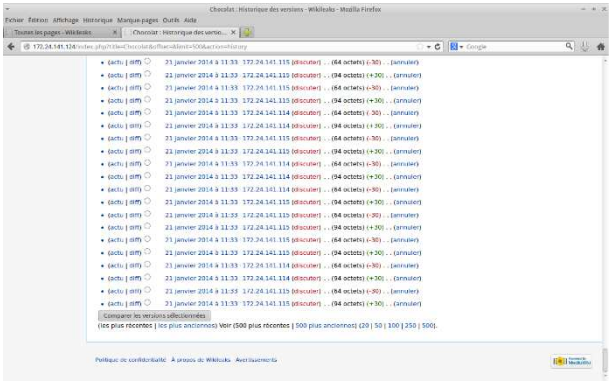
Screen 4

Page Chocolat avec la "tête de mort"



Screen 5

Historique de la page chocolat (début)



Screen 6

Historique de la page accueil (fin), on peut voir que l'historique s'arrête à 500, le reste a disparu

(Deux articles pour preuve, il n'est pas possible de tout mettre)

Information récupérée et/ou modifiées

Modification de tous les articles du wiki.

Comment s'en protéger?

- Désactiver l'API publique et la mettre en localhost, interdis pour le projet.
- Avoir un IPS qui bloque le robot: il est intelligent donc inutile.
- Bloquer l'API pour les gens non connectés: le bot peut se connecter donc inutile (il est facile d'automatiser la création d'un compte et de s'y connecter ensuite)
- Bloquer les IP qui font trop de demandes: oui mais il est possible de ralentir manuellement le robot