

2013/2014

M2-Informatique SSI

GULDNER Geoffrey

HURIER Médéric

LACAVE Valentin

SOIHILI Mouchtali



**[Rapport de défense
n°DXXX]**

SOMMAIRE

I. DESCRIPTION.....	3
A. N° D'ATTAQUE SUBIE	3
B. GROUPE AYANT REALISE L'ATTAQUE.....	3
C. DATE DE L'ATTAQUE.....	3
D. CATEGORIE D'ATTAQUE	3
E. TECHNIQUE UTILISEE	3
F. CID.....	3
II. DEGATS SUBIT	4
A. DESCRIPTION DES DEGATS	4
B. TRACES / PREUVES LAISSEES	4
III. CONTRE(S) MESURE(S) MISE(S) EN PLACE	4

I. Description

A. N° d'attaque subie

7^{ème} attaque sur notre serveur

B. Groupe ayant réalisé l'attaque

Les 4 zouaves de derrière

C. Date de l'attaque

30/02/9087

D. Catégorie d'attaque

Attaque DDOS

E. Technique utilisée

BotNet floodeur

F. CID

Disponibilité

II. Dégâts subit

A. Description des dégâts

Surcharge du serveur, rendu indisponible pendant 5 heures

B. Traces / Preuves laissées

Logs serveur

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

Refuser paquet syn tcp