2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport de défense n°D003]

SOMMAIRE

I. Description

N° d'attaque subie
Attaque n°1-2 sur notre serveur
Voir rapport de défense N°D001 et N°D002

Groupe ayant réalisé l'attaque
Groupe 2

- DEBUF-KAISER-JANATI-DEBRA (identifié grâce à l'adresse IP: 172.24.141.103)

Date de l'attaque
Voir rapport de défense N°D001 et N°D002

Catégorie d'attaque
Voir rapport de défense N°D001 et N°D002

Technique utilisée
Voir rapport de défense N°D001 et N°D002

CID
Voir rapport de défense N°D001 et N°D002

II. Dégâts subit

Description des dégâts
Voir rapport de défense N°D001 et N°D002

Traces / Preuves laissées
Voir rapport de défense N°D001 et N°D002

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

Ce rapport est écris pour vous informer de la contre mesure mise en place pour les attaques 1 et 2 subies. Elle se situe surtout pour toute attaque de type Dos. La contremesure mise en place est l'installation de Fail2Ban qui n'a pas été installé auparavant. Cela va permettre de bloquer les IP qui attaquent trop. Nous avons réglés le ban sur 300 secondes (5 minutes).