

Sécurité informatique, pas qu'une affaire de Geeks

Jérémy B.

2012

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Menaces virales

Comment s'en protéger ?

Attaques informatiques

Prise de contrôle, et autre hack

Attaque DOS

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

- ▶ « Je connais les droits et devoirs indiqués dans la charte d'usage des TIC de mon école » ;

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

- ▶ « Je connais les droits et devoirs indiqués dans la charte d'usage des TIC de mon école » ;
- ▶ « Je respecte les autres et je me protège moi-même dans le cadre de la communication et de la publication électronique » ;

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

- ▶ « Je connais les droits et devoirs indiqués dans la charte d'usage des TIC de mon école » ;
- ▶ « Je respecte les autres et je me protège moi-même dans le cadre de la communication et de la publication électronique » ;
- ▶ « Si je souhaite récupérer un document, je vérifie que j'ai le droit de l'utiliser, et à quelle condition » ;

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

- ▶ « Je connais les droits et devoirs indiqués dans la charte d'usage des TIC de mon école » ;
- ▶ « Je respecte les autres et je me protège moi-même dans le cadre de la communication et de la publication électronique » ;
- ▶ « Si je souhaite récupérer un document, je vérifie que j'ai le droit de l'utiliser, et à quelle condition » ;
- ▶ « Je trouve des indices avant d'accorder ma confiance aux informations et propositions que la machine me fournit ».

Avant de commencer

Cette présentation est en vue de valider quatres compétences du B2I, qui sont :

- ▶ « Je connais les droits et devoirs indiqués dans la charte d'usage des TIC de mon école » ;
- ▶ « Je respecte les autres et je me protège moi-même dans le cadre de la communication et de la publication électronique » ;
- ▶ « Si je souhaite récupérer un document, je vérifie que j'ai le droit de l'utiliser, et à quelle condition » ;
- ▶ « Je trouve des indices avant d'accorder ma confiance aux informations et propositions que la machine me fournit ».

Ainsi que de sensibiliser à la sécurité informatique.

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Il en existe plusieurs sortes :

- ▶ Les virus ;

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Il en existe plusieurs sortes :

- ▶ Les virus ;
- ▶ Les vers ;

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Il en existe plusieurs sortes :

- ▶ Les virus ;
- ▶ Les vers ;
- ▶ Les chevaux de Troie ;

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Il en existe plusieurs sortes :

- ▶ Les virus ;
- ▶ Les vers ;
- ▶ Les chevaux de Troie ;
- ▶ Les spywares.

Menaces virales

Les menaces virales sont les plus répandus, et ce sont celles qui peuvent faire beaucoup de dommages. Elles sont autonomes, une fois créés, elles n'ont pas besoin d'actions de leurs créateurs.

Il en existe plusieurs sortes :

- ▶ Les virus ;
- ▶ Les vers ;
- ▶ Les chevaux de Troie ;
- ▶ Les spywares.

Même fonctionnement qu'un virus biologique : contamination, infection.

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Le plus efficace est de ne pas en attraper, en restant prudent.

Voici quelques gestes pour limiter ces virus :

- ▶ Faire attention où l'on télécharge un fichier ;

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Le plus efficace est de ne pas en attraper, en restant prudent.

Voici quelques gestes pour limiter ces virus :

- ▶ Faire attention où l'on télécharge un fichier ;
- ▶ Utiliser de vrais navigateurs ;

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Le plus efficace est de ne pas en attraper, en restant prudent.

Voici quelques gestes pour limiter ces virus :

- ▶ Faire attention où l'on télécharge un fichier ;
- ▶ Utiliser de vrais navigateurs ;
- ▶ Maintenir ses logiciels à jour ;

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Le plus efficace est de ne pas en attraper, en restant prudent.

Voici quelques gestes pour limiter ces virus :

- ▶ Faire attention où l'on télécharge un fichier ;
- ▶ Utiliser de vrais navigateurs ;
- ▶ Maintenir ses logiciels à jour ;
- ▶ Rester prudent.

Comment s'en protéger ?

Dans l'absolu, la solution la plus fiable est de posséder un antivirus, tel que Avast !, Avira, MSE, etc...

Le plus efficace est de ne pas en attraper, en restant prudent.

Voici quelques gestes pour limiter ces virus :

- ▶ Faire attention où l'on télécharge un fichier ;
- ▶ Utiliser de vrais navigateurs ;
- ▶ Maintenir ses logiciels à jour ;
- ▶ Rester prudent.

La solution extrême consiste à changer pour un système où il n'y a pas de virus (Distribution Linux, Système Unix), mais ça peut être contraignant.

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Le protagoniste de cette attaque peut prendre le contrôle d'un PC pour le pire, ou bien voler des données, en supprimer, voler des mots de passe...

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Le protagoniste de cette attaque peut prendre le contrôle d'un PC pour le pire, ou bien voler des données, en supprimer, voler des mots de passe...

Pour s'en protéger, il faut :

- ▶ Être équipée d'un pare-feu (installé par défaut dans les versions récentes de Windows) ;

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Le protagoniste de cette attaque peut prendre le contrôle d'un PC pour le pire, ou bien voler des données, en supprimer, voler des mots de passe...

Pour s'en protéger, il faut :

- ▶ Être équipée d'un pare-feu (installé par défaut dans les versions récentes de Windows) ;
- ▶ Maintenir ses logiciels à jour ;

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Le protagoniste de cette attaque peut prendre le contrôle d'un PC pour le pire, ou bien voler des données, en supprimer, voler des mots de passe...

Pour s'en protéger, il faut :

- ▶ Être équipée d'un pare-feu (installé par défaut dans les versions récentes de Windows) ;
- ▶ Maintenir ses logiciels à jour ;
- ▶ Ne pas donner les droits administrateur à n'importe quel logiciel qui le demande.

Prise de contrôle, et autre hack

Cette menace consiste à attaquer manuellement une cible pré-définis, en profitant d'une faille de sécurité (aussi appelé Backdoor).

Le protagoniste de cette attaque peut prendre le contrôle d'un PC pour le pire, ou bien voler des données, en supprimer, voler des mots de passe...

Pour s'en protéger, il faut :

- ▶ Être équipée d'un pare-feu (installé par défaut dans les versions récentes de Windows) ;
- ▶ Maintenir ses logiciels à jour ;
- ▶ Ne pas donner les droits administrateur à n'importe quel logiciel qui le demande.

En général, ce sont plus les professionnels qui sont visés par ce genre d'attaque.

Attaque DOS

DOS = Denial of service (Déni de service). Celà consiste à saturer une machine (généralement un serveur) de sorte à ce qu'il ne puisse plus répondre et "crash".

Sécurité
informatique, pas
qu'une affaire de
Geeks

Jérémy B.

Avant de
commencer

Menaces virales

Comment s'en protéger ?

Attaques
informatiques

Prise de contrôle, et autre
hack

Attaque DOS

Attaque DOS

DOS = Denial of service (Dénî de service). Celà consiste à saturer une machine (généralement un serveur) de sorte à ce qu'il ne puisse plus répondre et "crash".

C'est la technique qu'utilisent les anonymous afin de protester sur le Net.

Ils le font grâce à un petit logiciel appelé LOIC (Low Orbital Ion Canon).