

L'utilisateur : L'ultime menace ?

Eric WIES

GS DAYS 2010

30 novembre 2010

L'utilisateur : l'ultime menace ?

- Les menaces et les protections
 - Virus, Spam, Pertes de données
- Tout va bien ?
- Cas réels et cas simulés
 - Quelques problèmes issus de l'utilisateur
- Et maintenant ?

Menaces : VIRUS



Menaces : SPAM

The image displays two overlapping Mozilla Firefox browser windows. The left window shows the 'Signal Spam' website, which is a national platform for reporting spam. The right window shows the 'SpamCop.net' website, which provides services for reporting spam and blocking it.

Signal Spam - Mozilla Firefox

signal spam

Accueil S'inscrire

Signalez vos spams d'un simple clic

Grâce à Signal Spam, il vous suffit d'un simple clic sur les spams que vous recevez, et obtenir un suivi de votre action.

Pour commencer dès maintenant, inscrivez-vous en utilisant le plug-in.

>> S'INSCRIRE

Plate-forme nationale de signalement des spams

Le projet de plate-forme nationale de signalement des spams est porté par une association de loi 1901.

Terminé

SpamCop.net - Beware of cheap imitations - Mozilla Firefox

http://www.spamcop.net

Help | Site Map | Text size: - +

Report Spam Filtered Email Blocking List Statistics Login

SpamCop is the premier service for reporting spam. SpamCop determines the origin of unwanted email and reports it to the relevant Internet service providers. By reporting spam, you have a positive impact on the problem. Reporting unsolicited email also helps feed spam filtering systems, including, but not limited to, SpamCop's own service.

Beware of Cheap Imitations

ESTABLISHED 1998

REPORT SPAM
Report spam to help Internet providers cut spam off at the source.
[Register Now](#)

GET SPAM-FREE EMAIL
Professional-grade SpamCop email accounts feature spam reporting, customizable spam and virus filtering and simultaneous Webmail, POP and IMAP access.
[Learn More](#)

USE FREE BLOCKING LIST
Use the SpamCop DNS-based Blocking List with your own mailserver and get safe and effective spam filtering for free.
[Learn How](#)
[Legal / Technical description](#)

REPORTED FOR SPAMMING?
Find out about SpamCop reports and spam blocking, email deliverability problems and what you can do to ensure that your mail will get through.
[Learn More](#)

GET HELP
Get information from SpamCop's extensive FAQ and active user community.
[Help Home](#)

NEWS: Postmasters, please limit forgery blow-back:
Delayed bounces, virus notices, vacation messages [More..](#)

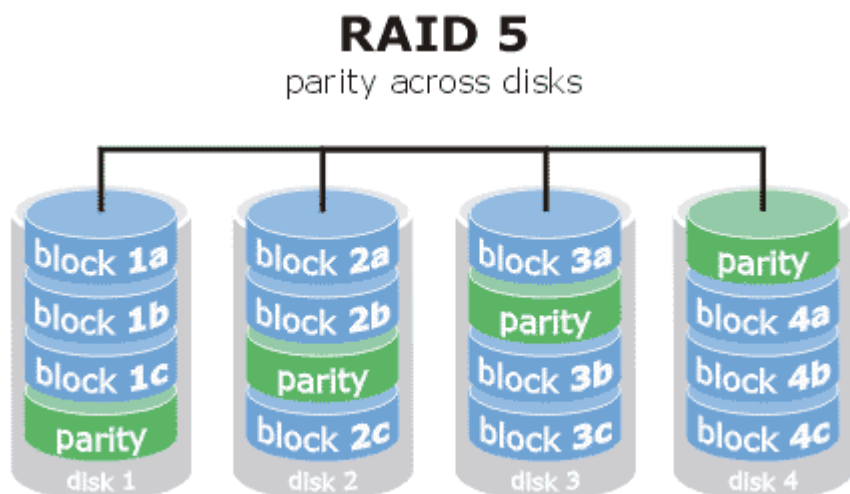
©1992-2010 Cisco Systems, Inc. All rights reserved. [HTML4](#) / [CSS2 Firefox](#) recommended - [Policies and Disclaimers](#)

Terminé

Options x

Apache/2.0.63 100%

Menaces : Pertes de données



1st Full Backup



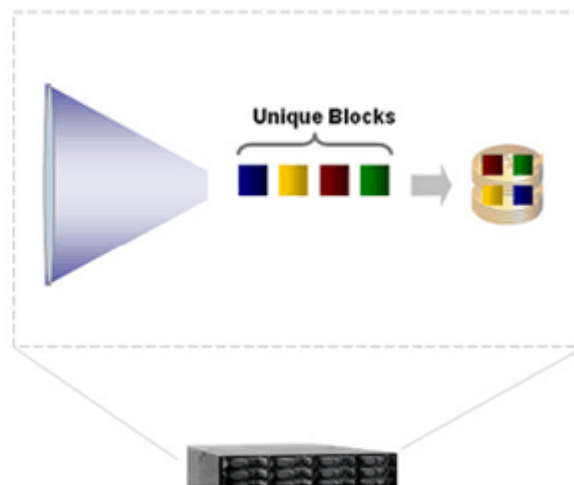
2nd Full Backup



3rd Full Backup



4th Full Backup



Menaces :

Intrusions dans les réseaux



Menaces : Intrusions physiques



Eric WIES - GS DAYS 2010 -
L'utilisateur l'ultime menace ? 30 novembre 2010

Protection des données personnelles



Des instances

- DSI
 - Direction de la sécurité de l'information
- RSSI
 - Responsable de la sécurité de l'information
- CIL
 - Correspondant informatique et liberté
- Le tout pour aboutir à la sécurité maximum
 - PRA/PCA

Des recours légaux



ANSSI

Agence nationale de la sécurité des systèmes d'information





ALORS TOUT VA BIEN ?

Cas réel :

Changement de photocopieur

- Le fournisseur de photocopieurs demande
 - Login et mot de passe de l'administrateur
 - Pour permettre au technicien d'intervenir
- L'opérateur remplit le document
- Mais ne le renvoie pas
 - Il demande le support du service informatique
 - Car il ne connaît pas le mot de passe !

Cas réel : Banque de France



- Contrat de travail de BDF
 - Demande de la discrétion
- Utilisation de l'internet dans la BDF
 - Interdiction d'utiliser les réseaux sociaux
- Mais sur les réseaux sociaux
 - Très grands nombres de personnes
 - On trouve leurs données personnelles
 - Adresse, famille, loisirs
 - Et leur progression dans la BDF

Cas réel :

Cour d'appel de Metz

- L'entrée est restreinte
 - pour les visiteurs
- Mais non contrainte
 - pour les personnels
- On peut trouver
 - Les personnels,
 - Leur adresse,
 - leurs hobbies,
 - Leurs fonctions dans la cour d'appel
- Comment entrer dans la cour d'appel ?
- Comment faire entrer un matériel ?



Cas réel :

Visite d'une usine

- Usine d'un grand constructeur informatique
- Tous les travailleurs sont contraints
 - Portiques, fouilles, vidéo surveillance
- Mais les visiteurs gardent leur téléphone
 - Enregistrement de son
 - Photos, Vidéos
 - Et le tout sur internet en temps réel !

Cas réel :

Propagation d'un virus

- Un étudiant apporte une clé USB
 - Clé semblant défectueuse
- L'enseignant la connecte
 - Sur son poste
- Puis l'essaye
 - Sur les postes de ses collègues
- Quand 5 postes sont essayés
 - On se tourne vers les équipes informatiques
 - Mais le virus est déjà présent et actif !



Cas réel :

MI 5

- Futur directeur du MI 5
 - Spécialiste de la sécurité de l'information
 - Contraint à la démission (mai 2009)
- Photos personnelles sur FaceBook
 - Diffusées par sa femme !

Cas réel :

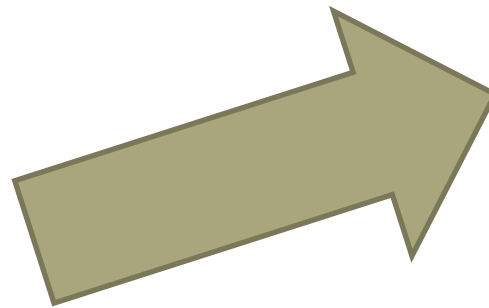
Dénigrement

- Michelin, Cholet 2008
 - Licenciement pour dénigrement
- Licencié pour
 - Avoir rempli sa page Facebook
 - Pendant un congé maladie
- Licencié pour
 - Avoir dénigré ses collègues
- Photos et Vidéos volées
 - Surtout des enseignants !

Cas réel :

Vie d'entreprise / privée

- Téléphone d'entreprise
 - Ligne d'entreprise
- Mais terminal personnel !
- Mélange des données !



Cas réel :

Utilisation de Yahoo Groupes

- Les plates formes d'entreprise
 - Sont réglementées
 - Sont contraintes
 - Nécessitent des accords
- Les plates formes communautaires
 - Utilisables facilement
 - Sans contrainte
 - Sans limite !
- Appartenance des documents?



Cas réel : Installation d'un faux logiciel

VLC - Mozilla Firefox

http://browserdrl.com/VLC/?ref=172878

Alerte WOT : ce site a mauvaise réputation.

VLC MEDIA PLAYER

Télécharger VLC PLAYER
Installation rapide et gratuite

VLC Media Player, le lecteur multimédia le plus utilisé au monde !

VLC est gratuit
VLC est un logiciel GRATUIT, distribué sous licence publique générale (GPL) GNU.

Fonctionne avec tous les formats multimédia
VLC supporte tous les formats multimédia, même les fichiers endommagés, sans avoir besoin de codecs ou plugins supplémentaires.

Serveur streaming inclus
VLC inclus un serveur streaming complet en continu, avec fonctionnalités ajoutées comme la vidéo sur demande, le transcodage en temps réel, et plus encore.

POURQUOI TÉLÉCHARGER VLC ?

- Nouveaux HD codecs (AES3, Dolby Digital Plus, TrueHD, Blu-Ray Linear PCM, Real Video 3.0 et 4.0, ...)
- Nouveaux formats (Raw Dirac, MZTS, ...)
- Enregistrement live
- Contrôles de vitesse plus précis
- Gratuit et Open Source
- Indépendant des systèmes codecs
- Serveur Streaming
- Vidéo sur demande
- Qualité vidéo et audio supérieure
- Exige moins de ressources que Windows Media

TÉLÉCHARGER VLC MEDIA PLAYER MAINTENANT

JavaScript actuellement interdit | <SCRIPT>:2 | <OBJECT>:0

Terminé

VideoLAN - VLC media player - Open Source Multimedia Framework and Player - Mozilla Firefox

http://www.videolan.org/vlc/

VideoLAN Project | VLC media player | Software Projects | Doc/Support | Wiki | Forum | Developers

VideoLAN

Download | Features | Screenshots | Streaming | Skins

VLC: open-source multimedia framework, player and server

VLC media player
VLC is a powerful media player, playing most of the media codecs and video formats out there.

Open Source
Trust your multimedia software and codecs, all VideoLAN projects are **free** and **open source**.
[More about Open Source](#)

Volunteers Organization
VLC and VideoLAN are projects, composed of volunteers, developing and promoting **free multimedia solutions**.
[More about VideoLAN](#)

Versatile media player | Skinnable interface | Full streaming server | Powerful media converter

"It plays everything!"

The media player that fills all your needs. It can handle DVDs, (S)VCDs, Audio CDs, web streams, TV cards and much more.

You don't need to keep track of a dozen codec packs you need to have installed. VLC has all codecs built-in. It comes with support for nearly all codec there is.

And what is more it can even play back the file or media if it is damaged! Missing or broken pieces are no stop to VLC, it plays all the video and audio information that's still intact.

[View all supported formats](#)

Download VLC
Windows, 18 MB | [Other Systems, Versions](#)

Get VLC now!

Binaries
Select your operating system to download VLC binaries:

- Windows | Syllable
- Mac OS X | iOS

GNU/Linux

- Debian GNU/Linux | Red Hat Enterprise Linux
- Ubuntu | Slackware Linux

VLC 1.0 downloads: **176,973,992**
0.1 downloads per second
[Full statistic](#)

Features
For more information about what features are supported on your operating system, please see the [full features list](#).
You can also have a look at some [VLC](#)

Terminé

88.191.250.2

Cas simulé :

Collecte d'informations



- Action Discrète – 21 nov 2010
- Groupe humoristique de Canal +
 - Propose une vidéo (en caméra cachée)
- <http://www.canalplus.fr/c-humour/pid1780-c-action-discrete.html>
- Google Inside
 - Cartographie de l'intérieur des bureaux
- Mesure d'hygrométrie
 - Place un enregistreur dans une salle de réunion
- Père Noël
 - Offre une clé USB à chaque journaliste !

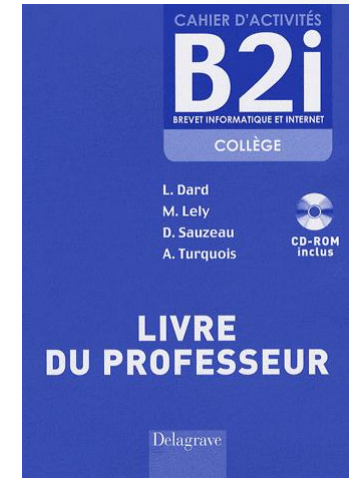
QUE FAIRE ?

Reprendre le contrôle

- L'utilisateur
 - Devient force de propositions
 - Ne joue plus à cache-cache
- Les équipes informatiques
 - Intègrent les usages privés
 - Dans les choix d'architecture !
- Formation des utilisateurs
 - À la réglementation
 - Aux risques

Informer/ Former

- Depuis le collège, lycée
 - B2I, C2I
- Jusqu'à l'université
 - Formation aux risques de la fuite d'information
- Mais aussi
 - Formation continue/ d'entreprise
 - Conférences/ Associations
- But :
 - Répandre les bonnes pratiques
 - Expliquer les conséquences



Conclusion

- La sécurité de l'information
 - Concerne tout le monde
 - Y compris (et surtout) le grand public !
- Les équipes informatiques et les utilisateurs
 - Doivent travailler ensemble
 - Pour anticiper les usages
 - Sans mettre en danger l'entreprise !

Questions ?