

2€
SEULEMENT

**PRENEZ
LE CONTRÔLE
D'UN ORDINATEUR
À DISTANCE !**

✂ EXCLUSIF WIKILEAKS : QUI SONT SES SOURCES ?

COMMENT ELLES TRANSFÈRENT DES
DONNÉES CRYPTÉES.
COMMENT WIKILEAKS LES PROTÈGE.
LE PENTAGONE VEUT LEURS TÊTES.

✂ DANGER

PETITS GUIDES DU CHIMISTE
AMATEUR : ILS FABRIQUENT DE
LA DROGUE SUR INTERNET !

✂ HACKING

PIRATAGE DE MOBILES GSM :
ILS SAVENT OÙ VOUS ÊTES ET
CE QUE VOUS FAITES

SÉCURISEZ VOTRE CLÉ USB

PIRATAGE DE COMPTE
FACEBOOK

**MODIFIEZ VOTRE VOIX AU
TÉLÉPHONE**

TOUT SAVOIR SUR L'ART
DE LA STÉNOGRAPHIE

**100%
INFOS
0% INTOX !**

MOTS DE PASSE, ANONYMAT, CRACKS,
BASES DE DONNÉES, IPAD,
GOOGLE, PROTECTION, JAILBREAK,
SOCIAL ENGINEERING, WI-FI...



LE 1^{ER} MAGAZINE BITTORRENT

NOUVEAU !

LE MAGAZINE 100% PRATIQUE BITTORRENT ET P2P

Bitorrent

MAGAZINE

BEST-OF 2010

SOI E04 • AOÛT/OCTOBRE 2010

LE TOP 10 DES NOUVEAUTÉS BITTORRENT

100% PRATIQUES & GRATUITS P.10

**LES 10 SERVICES
ET LOGICIELS
QUI RÉVOLUTIONNENT
VOS TÉLÉCHARGEMENTS**
► BTaccel, Put.io, Foofind,
Torrindex, Tribler, Leechpack,
Plugins pour Firefox, etc!

GUIDE PAS À PAS

COMMENT ÇA MARCHE ?

- Plus de limites sur MEGAVIDEO P.23
- CONVERTIR toutes vos vidéos P.28
- ACHATS ET LOCATIONS DE JEUX
sur Internet : LES BONS PLANS P.26
- ANONYMAT FACILE avec Tor P.29
- Générateur de CLÉS WI-FI ! P.29



MEGAUPLOAD P.24

Les meilleurs sites
pour **TÉLÉCHARGER**
SUR MEGAUPLOAD



*L'avenir du numérique chez votre
marchand de journaux*

PIRATE INFORMATIQUE

100% LIBRE

PAGE 08-09

**La Chine s'éveille !
Entre l'Empire du Milieu et
Google, rien de va plus ?**



PAGES 10-11

**Le Social Engineering
ou l'art de la
tromperie.
Obtenez des
informations sans
toucher d'ordinateur !**



**Ils fabriquent de
la drogue !
Les sites qui
donnent les
«recettes»...**



PAGES 12-13

**ATTENTION AUX GSM :
VOUS ÊTES FLIQUÉS !**



PAGE 14-15

PAGE 19

**WIKILEAKS :
la liberté d'expression
en danger ?**



PAGES 22-23

**L'art de dissimuler
des informations :
la stéganographie.**



PAGES 24-25

**Moduler sa voix : c'est
possible et ça peut
rapporter gros...**



PAGES 26-27

**Prise de contrôle
à distance :
quand se
déplacer ne
sert à rien !**



PAGES 16-17

**Les nouveaux
outils pour pirater
les bases de
données**



PAGES 20

**Protégez vos
clés USB !**



PAGES 21

**Les zones sensibles
de votre Facebook**



Nos MICRO-FICHES :

**Les meilleures
astuces de la
rédaction !**



PAGES 28-29

13 millions de PC zombie orphelins

Le «créateur» du gigantesque botnet Mariposa a été arrêté ! Il s'agissait d'un Slovène de 23 ans qui, non content d'avoir créé ce gigantesque réseau de PC zombie, vendait aussi une solution clé en main pour que ses «clients» puissent en faire de même. Fort de 13 millions de machines contaminées, Mariposa a servi à pirater des cartes bancaires et des comptes en ligne de 500 grandes entreprises et 40 banques. Maintenant que «l'iserdo» est sous les verrous, Mariposa devrait disparaître puisqu'il lui est impossible de mettre son logiciel à jour. La tâche est cependant énorme puisque la plupart du temps les utilisateurs débutants ignorent que leur machine est infectée...



StarCraft II gratuit ?

Douze ans après la sortie du premier volet, StarCraft II est en quelques semaines devenu un blockbuster que les utilisateurs de PC attendaient de pied ferme. Il n'en fallait pas plus pour que des petits malins exploitent ce phénomène. Attention donc aux emails qui circulent actuellement et dont le but est de mettre la main sur le compte Battle.net des joueurs. Ce phishing envoyé depuis une adresse du type «@blizzard.review.com» propose une clé gratuite à tout possesseur d'un compte Battle.net. Quoique très ciblé, ce piège devrait tout de même faire des victimes. Prudence...



Vi4gr4 ch3r & p4s b0n...

Selon le magazine Test-Achats, la moitié des médicaments vendus sur Internet sont contrefaits ! Pire encore puisque dans un récent communiqué, le site indique qu'ils sont plus chers que dans les pharmacies. Pour réaliser son test, le magazine a commandé sur différents sites trois médicaments délivrés uniquement sur ordonnance : le Xenical (pour la perte de poids), le Tramadol (analgésique) et le Viagra (qu'on ne présente plus). Lors de la commande, les sites demandent à ce que le «patient» remplisse un formulaire médical et à chaque fois les testeurs inséraient une affection incompatible avec la commande (personne cardiaque qui commande du Viagra, par exemple). Or sur les 16 commandes passées, 11 ont été acceptées et seulement 9 ont été livrées (dont 2 sans notice et sans la boîte d'origine). En moyenne, le prix des médicaments commandés est 34,5 % plus cher qu'en pharmacie.

Ils font le bonheur des pros

Caméras cachées, micros invisibles... Désormais, grâce à Internet, le matériel d'espionnage professionnel est exposé à la convoitise de tous. James Bond, François Mitterrand et Richard Nixon les auraient réclamés !

Porte-clés caméra

Disponible en version 4 et 8 Go, cette caméra enregistre le son et la vidéo d'une simple pression de bouton. Se dissimulant sous des airs de porte-clés, il est possible de la laisser dans une pièce en votre absence ou la garder en main. Il est possible de paramétrer l'appareil pour qu'il prenne des photographies à intervalle régulier. Pas de problème pour récupérer les données

puisque vous pourrez le connecter sur un simple port USB...

Prix : 49 €

 www.top-espion.com



Micro discret

De la taille d'une clé USB, cet enregistreur audio numérique permet d'espionner sans se faire remarquer. Doté d'une fonction d'enregistrement directe par simple pression d'un bouton, l'appareil est aussi doté de nombreuses fonctions qui le rend polyvalent : trois modes de qualité audio différents, activation vocale pour enregistrer seulement quand il y a une conversation dans la pièce où vous l'avez placé, micro interne et micro cravate, réduction du bruit ambiant, etc. Sa mémoire interne de 2 Go permet de stocker jusqu'à 560 heures d'enregistrements.

Prix : 149 €

 www.espion-on-line.com



WifiRobin, paré à cracker !

Nous vous avons déjà parlé du WiFi-Box, un dispositif venu de Malaisie qui permettait «d'emprunter» la connexion du voisin grâce à l'application Back-Track. À la fois utilisé pour pirater les réseaux Wi-Fi mal protégés et éviter de tomber dans les mailles du filet HADOPI, ce genre d'appareil fait des émules puisque depuis peu de temps, la société espagnole WifiRobin propose un boîtier embarquant directement le logiciel qui permet d'analyser et de cracker les clés de chiffrement. Doté d'une antenne surpuissante (5 dBi au lieu de 2 dBi pour la WiFi-Box), ce WifiRobin détecte un grand nombre de réseaux Wi-Fi dans un rayon de 2 kilomètres et permet de contourner en vingt minutes les protections WEP (64, 128 et 152 bits), WPA 802.1X, TKIP et AES. Le taux de transfert est de 54 Mbps, l'appareil est auto-alimenté par port USB et est bien sûr compatible avec tous les Windows ainsi que les Mac et Linux. Pour la modique somme de 120 €, vous pourrez donc vous amuser à tester la connexion de vos chers voisins. Attention, ce genre de sport peut vous attirer des ennuis : 30 000 € d'amende et 2 ans de prison si le voisin en question n'est pas au courant...



JAIL-BREAK FACILE !

Depuis la légalisation du déblocage des téléphones par les États-Unis, les choses semblent s'accélérer du côté des logiciels de jailbreaking. Dorénavant, il existe même un service uniquement disponible en ligne. Compatible avec les appareils tournant sous iOS 4 (iPhone, iPad et iPod Touch), JailBreakMe ne nécessite pas d'ordinateur pour procéder à cette manipulation (qui consiste en fait à pouvoir installer des applications non signées). Il suffit de se connecter à www.jailbreakme.com depuis son téléphone. Comme son grand frère, JailBreakMe exploite une faille d'iOS par l'intermédiaire du navigateur Safari. Attention, si vous tentez une telle opération veillez à bien sauvegarder vos données...



À la trace

Voici un enregistreur de position GPS très compact (47x38x13 mm) très facile à utiliser. Une fois activé, il enregistre les positions GPS. Il peut être mis sur un porte-clés ou dissimulé dans un véhicule. Vous pourrez, par exemple, retracer une randonnée, l'itinéraire d'un véhicule, d'une personne, etc. Une fois récupéré, connectez-le à votre PC et téléchargez via son câble USB les itinéraires enregistrés. Pour visualiser la position sur une carte ou une image satellite, le service Google MAP est gratuit !

Prix : 59 €

 www.top-espion.com



Access denied

Appelée Pledge, cette poignée de porte intègre un verrou avec lecteur d'empreintes digitales. Ce solide petit système biométrique permet de s'assurer de la sécurité de votre vie privée. Idéal pour protéger une pièce de votre appartement ou votre garage, le dispositif fonctionne avec 4 piles AA et reste très facile à utiliser. Il est possible de programmer jusqu'à 120 empreintes digitales pour garantir l'accès à vos collègues, amis, etc.

Prix : 200 €

 <http://toutpourvous0.surinternet.com>



Bye bye Jiwa...

Un des pionniers du streaming musical en ligne vient de disparaître. En effet, Jiwa n'est plus depuis le 4 août dernier. En liquidation judiciaire, la société n'a pas pu faire face à la concurrence d'Apple, aux téléchargements illégaux (qui représentent toujours une part importante de la consommation de musique sur Internet) et à la cupidité des majors. En effet, les sommes que Universal Music, Warner Music, EMI ou Sony Music exigeaient pour que Jiwa puisse se targuer d'être un service légal étaient bien au-dessus des revenus du site. Pour 2009, la société avait dû verser 1 million d'euros alors que le chiffre d'affaire n'était que de 300 000 €... Et lorsque Jiwa a commencé à préparer une version



payante pour booster un peu ses chiffres, les majors ont immédiatement demandé encore plus d'argent. Équation impossible pour cette petite entreprise... De même, Jiwa comptait beaucoup sur «Carte musique jeune» (une initiative gouvernementale qui devait octroyer 50 € de bon d'achat aux jeunes pour acheter de la musique en ligne) qui devait être lancée au début de cette année mais qui a été repoussée à l'automne prochain. Pas de place pour les «petits» dans ce monde de «majors»...

SOURIEZ, VOUS ÊTES FILMÉS !

Les chiffres d'un récent rapport de la Chambre Régionale des Comptes de Rhône-Alpes sur la sécurité publique à Lyon ne parlent pas vraiment en la faveur des caméras de surveillance. En effet, cette analyse sérieuse montre que dans la Capitale des Gaules, les caméras de vidéosurveillance permettent une arrestation par caméra et par année. C'est ainsi que l'on apprend que les 219 caméras qui surveillent la ville n'ont permis l'arrestation que de 200 personnes. Quand on sait que sur une année, Lyon compte plus de 20 000 actes de «délinquance de voie publique», on peut se poser des questions sur l'utilité de ces caméras, qui, en plus de coûter une fortune aux contribuables, posent le problème de la protection de la vie privée. Pour le gouvernement pourtant, la multiplication des caméras permettrait une baisse de la délinquance. Or, toujours selon ce même rapport, l'impact n'est pas aussi net. En effet, même si entre 2003 et 2008, la délinquance a baissé de 33 % à Lyon, elle a baissé de 48 % chez la voisine Villeurbanne où aucune caméra n'est installée. On fait dire aux chiffres ce que l'on veut...

Plus de BlackBerry dans les pays totalitaires ?

Suivant l'exemple des Émirats Arabes Unis, l'Arabie Saoudite a suspendu les services des BlackBerry (tchat, e-mails et la recherche sur Internet). En effet, le fabricant canadien Research in Motion (RIM) ne souhaite pas partager les secrets de son algorithme de cryptage unique. Il faut savoir que lorsque vous envoyez un email, les données transmises par les BlackBerry transitent par les serveurs de RIM pour y être chiffrées ou déchiffrées. Pour les gouvernements, il n'est alors plus possible de surveiller les données réceptionnées ou émises par ces téléphones. Pour ces pays du Golfe persique, il s'agit officiellement d'un problème de sécurité nationale mais pour les organismes non gouvernementaux, il s'agit avant tout de censurer le Net. Le problème très épineux puisque ce sont plus de 500 000 clients aux Émirats Arabes Unis qui pourraient se retrouver avec un BlackBerry sans

aucun intérêt (à part celui de téléphoner bien sûr). L'Inde a aussi dernièrement demandé à avoir un accès aux données mais pour ce pays, RIM a trouvé un compromis avec le gouvernement. La société a proposé de fournir aux services de renseignement indiens les codes nécessaires pour avoir accès aux e-mails des entreprises et des particuliers limités dans le temps. C'est peut-être le début de la fin pour la méthode de chiffrement de RIM puisqu'on voit mal comment la société pourrait dire non aux Émirats Arabes Unis et à l'Arabie Saoudite. De même, les Canadiens qui viennent d'ouvrir leur première boutique en Chine devront sans doute mettre de l'eau dans leur Tsingtao...



LE MAGAZINE NOUVELLE GÉNÉRATION

CLICK & LOAD

N°11 TÉLÉCHARGEMENT & STREAMING

Mai/Juin 2010



2€
50

12 LOGICIELS
POUR DOPER
VOTRE **WEBCAM**

HADOPI : LA CHASSE AU PIRATE EST OUVERTE

LES 10 SOLUTIONS QUI ÉCHAPPENT À LA SURVEILLANCE



Films, musique, jeux :
LES SERVICES QUI PROMETTENT
L'IMPUNITÉ AUX INTERNAUTES

DOSSIER **MUSIQUE**

MP3 & Playlists

Tout copier, transférer,
tagger et mixer !

EMULE 0.50a

Les secrets
de la nouvelle
version !



EXCLUSIF

Google TV

La télé 2.0
arrive enfin !

100% PRATIQUE

[BitSnoop] [Devenez producteur de cinéma]
[Regardez et enregistrez la télé de rattrapage]
[Les Serious Games, c'est sérieux !] [µTorrent]

EN KIOSQUE

NOUVEAU !



La Chine s'éveille !

Depuis le début de l'année, nous avons été témoin du bras de fer entre la République Populaire de Chine et Google. Entre hacking, menaces, soupçons et réconciliation, revenons sur ces événements pour le moins particuliers...



Lancé en grande pompe en 2006, Google.cn a immédiatement essuyé des critiques de la part des opposants au régime chinois et des organisations non gouvernementales. À l'instar de Microsoft et Yahoo, ces derniers lui reprochaient d'accepter le «filtrage des contenus», une censure visant à mettre un mur entre l'internet des chinois et l'internet du reste du monde.

Il suffisait de taper «Tien'anmen» sur le Google chinois pour se rendre compte que les résultats qui s'affichaient différaient de ce que l'on pouvait trouver ailleurs, tant au niveau des liens que des images... Pourtant le gouvernement chinois n'a pas facilité la tâche au géant de Mountain View puisque parfois, les services «made in» Google se voyaient coupés pour des raisons plus ou moins fantaisistes. La plupart du temps, le prétexte utilisé était la mise à disposition de contenus pornographiques (mouais...). Google s'accommodait de ces petits caprices jusqu'en mars dernier où la compagnie a eu une désagréable «visite» dans ses serveurs. Une attaque informatique venant de Chine et ayant «abouti à un vol de propriété intellectuelle» selon un des vice-présidents David

UNE LÉGÈRE DÉTENTE ?

Dernier rebondissement en date du côté de l'affaire «Google contre la Chine» : David Drummond s'est dernièrement félicité du renouvellement de la licence ICP (Internet Content Provider) qui permet aux sites d'opérer en toute légalité en Chine. Il faut dire qu'à part le moteur de recherche, toujours redirigé vers Hong Kong, les services Google (Gmail, etc.) sont disponibles depuis Google.cn. Pour la Chine, ce renouvellement implique que Google jouera le jeu. Wait and see...

i



Drummond. Après enquête de Google, il semblerait que d'autres sociétés évoluant dans les domaines d'Internet, des médias et de la technologie ont aussi été attaquées de la même manière. Pour Google, vu la débauche de moyen mis en œuvre, il ne peut s'agir d'un pirate isolé. Mais sans preuve, Google n'accuse pas implicitement le gouvernement chinois...

Pourquoi Google ?

Mais pourquoi une telle attaque ? Selon Google, le but des pirates était d'accéder aux comptes Gmail de certains militants chinois des droits de l'Homme. Heureusement les correspondances n'ont pu être piratées, seules des données non sensibles ont été compromises (diverses informations concernant les comptes, date de création, etc.) Mais le divorce est déjà à l'horizon. Suite à ces histoires, Google décide alors de «reconsidérer l'approche de la Chine» et de ne plus filtrer les résultats de recherche sur Google.cn. Plutôt courageux alors que Microsoft et Yahoo avaient courbé l'échine devant le formidable marché que représente la Terre du Milieu (plus de 350 millions d'internautes). En effet Google, leader des moteurs de recherche dans le monde n'est que numéro 2 en Chine où le moteur

local Baidu s'accapare près de 65 % des parts de marché.

La Chine s'offusque

Devant ces accusations à mots couverts, le porte-parole du ministère des Affaires étrangères chinois a déclaré que : «l'Internet en Chine est ouvert, que le gouvernement chinois encourage son développement et que la loi chinoise interdit toute forme de cyber-attaques». Il faut bien sûr comprendre : «On ne censure pas, on veut vraiment faire du business avec Internet et pour ce qui est des attaques, c'est pas nous !». Le gouvernement chinois n'en dit pas plus pour ne pas envenimer la situation. Il faut dire que même si Google n'est que numéro 2 avec un peu plus de 30% des parts de marché, la marque américaine est très connue même des non-internautes. Depuis les débuts du capitalisme dans ce pays, tout le monde - y compris les grands dirigeants mondiaux (suivez mon regard) - leur mange dans la main. Si Google ferme ses locaux, licencie ses 700 employés et dit au revoir au marché chinois, ce serait une sorte de camouflet pour le gouvernement de Pékin.

Statu quo ?

Depuis peu, Google est en partie passé à l'acte. Les internautes chinois qui se connectent sur Google.cn ne peuvent plus faire de recherches. Lorsqu'on clique dans le champ prévu à cet effet, nous sommes redirigés vers la version hongkongaise de Google, non censurée bien sûr (l'arrêt du filtre de censure sur Google.cn aurait été perçu comme une véritable déclaration de guerre pour les officiels chinois). La maison Blanche se dit «décue» qu'un accord



David Drummond a réussi son coup. Ni Google, ni la Chine ne perdent la face !

n'a pu être trouvé et Pékin trouve cette mesure «inamicale». La Chine rappelle d'ailleurs que «la seule condition de l'ouverture aux investissements étrangers est le respect des lois chinoises». Pourtant il serait facile aux chinois de bloquer l'accès à la version hongkongaise de Google. Il y a déjà eu des précédents pour YouTube et même avec le service Google Blogger (Ha, les chinois et la liberté d'expression !). Mais ici ce statu quo arrange tout le monde puisque personne ne perd vraiment la face. Google reste dans la place et compte bien faire travailler ses employés sur d'autres projets (comme Android) et le gouvernement chinois peut continuer de dire que toutes les entreprises étrangères qui ont des sites sur leur territoire respectent les lois. Il est aussi intéressant de noter que sur le blog de l'entreprise, David Drummond a pensé aux 700 employés chinois en précisant que «Toutes les décisions ont été inspirées et mises en œuvre par nos dirigeants aux États-Unis» (ici, il faut comprendre : «Ils n'y sont pour rien alors ne leur faites pas de mal, on ne paiera pas les exécutions !»).



Impossible de faire une recherche sur Google.cn depuis mars !



Social Engineering : l'art de la tromperie

Appelé ingénierie sociale en français, le social engineering est un ensemble de technique qui permet d'obtenir des informations auprès de personnes autorisées sans qu'elles se rendent compte de la supercherie. Pour arriver à ses fins le pirate va alors utiliser ses connaissances (pas forcément informatique), une dose de culot et sa capacité de persuasion...

Einstein disait «Deux choses sont infinies : l'Univers et la bêtise humaine. Mais, en ce qui concerne l'Univers, je n'en ai pas encore acquis la certitude absolue». En utilisant la bêtise, l'ignorance ou la crédulité de certaines personnes, il est possible d'obtenir ce qu'on veut. Pourquoi essayer de hacker un mot de passe s'il suffit de le demander «gentiment». Ce n'est pas aussi simple que cela mais en utilisant un peu sa tête, il est possible de faire croire à certaines situations. Il faut pour cela se mettre dans la tête de votre adversaire. La technique la plus facile passe par le téléphone : le but du pirate est d'avoir le renseignement le plus rapidement possible. Pour cela, il aura préparé son personnage, son discours et son «histoire». Il sera très persuasif dans le timbre de sa voix. Certains hackers ont quelques techniques pour parfaire leur crédibilité, comme posséder

un logiciel qui va générer des bruits de bureau ou qui va changer le timbre de la voix pour imiter celle d'une secrétaire par exemple (voir notre article page 24).

Hackons la rédaction...

Imaginons que vous souhaitiez connaître les chiffres de vente de ce magazine. Cette donnée confidentielle n'est connue que de très peu de personnes : le chef, quelques journalistes et le distributeur. Vous appelez à la rédaction pendant une période de vacances (les gens sont parfois partis et les stagiaires, même intelligents, ne sont pas forcément au courant de la confidentialité de certaines infos) et vous tombez sur un journaliste. En vous faisant passer pour quelqu'un de la distribution (le nom est écrit dans l'ours du magazine) vous lui faites croire qu'il y a un problème avec certains kiosques qui n'ont pas reçu les magazines (une catastrophe !)...

ID Presse : Ha mince combien de kiosque ?

Le pirate : Une centaine mais les magazines sont juste perdus, on va les retrouver ne vous inquiétez pas. Il nous faudrait juste le tirage exact pour redistribuer au mieux en attendant...

ID Presse : Quoi ? Mais vous n'avez pas cette information dans vos registres ?

Le pirate (prend l'air gêné) : Si mais nous avons un problème d'informatique ici et avec les vacances, vous savez ce que c'est...

ID Presse : Ok, le tirage pour ce numéro est de XX XXX exemplaires.

Le pirate (prend un air détaché et fait semblant de chercher dans des papiers, bruits de feuilles à l'appui) : Ha oui quand même



c'est pas mal en ces temps de crise mais vous devez avoir beaucoup d'invendu tout de même... [ici le pirate essaye d'obtenir les chiffres de vente en jouant sur l'orgueil du journaliste]

ID presse : Ho pas tant que ça vous savez, nous vendons à peu près ... Heu attendez, comment vous m'avez dit que vous vous appelez ?

Le pirate (sans se décontenancer) : Monsieur Y, je remplace Monsieur X pendant ses vacances [le pirate a été chercher sur Internet l'organigramme de la société].

ID Presse : Ha sacré Monsieur X, toujours fan du PSG ?

Le pirate : Oui, il a même renouvelé son abonnement au Parc !

Ici le pirate est démasqué puisque le journaliste sait pertinemment que Monsieur X est fan absolu de l'OM. La conversation s'arrête mais le pirate a quand même réussi à connaître le véritable tirage du magazine. Il persévère et appelle maintenant le distributeur...

Le pirate (d'un ton mécontent) : Bonjour c'est Monsieur Côme d'ID Presse, nous avons un

problème de comptabilité sur le mois de juin et ce n'est pas la première fois ! Qu'est-ce qui cloche chez vous enfin ?

Le distributeur : Ha je suis désolé, je remplace actuellement Monsieur X, je ne suis pas au courant...

Le pirate : C'est un scandale, nous ne sommes pas payés et vous n'êtes pas au courant !

Le distributeur (en panique car ID Presse est un bon client) : Le mois de juin vous dites ? Attendez je regarde...

Le pirate (qui utilise les données qu'il a obtenues auparavant pour se donner de la crédibilité) : Oui c'est celui du mois de juin avec un tirage de XX XXX exemplaires.

Le distributeur : C'est étrange, selon mes chiffres vous avez reçu X € pour la vente de XX XXX magazines [ça y est notre pirate a réussi son coup, il connaît maintenant les ventes du mois de juin et combien l'entreprise a touché pour ces ventes.]

Le pirate : Attendez c'est peut-être une erreur de notre part au niveau des dates. Selon vous combien avons-nous touché pour janvier, février, mars, avril et mai ?

Souvent, plus c'est gros et plus ça passe. Avec une simple règle de trois, notre pirate connaît maintenant les chiffres de vente des mois précédents...

Une seule parade : la paranoïa

Il existe aussi d'autres cas de figure. Par exemple, le pirate peut prendre contact avec la société par lettre : en-tête, logo et filigrane à l'appui. On peut aussi imaginer une boîte postale avec un nom d'emprunt pour sa société fictive. Via Internet, le pirate peut se faire passer pour un responsable informatique ou un ingénieur réseau dans l'espoir d'obtenir des informations sensibles. On peut aussi imaginer un contact direct. Ici les accessoires seront un costard-cravatte ou un bleu de travail en fonction de son «histoire». Le pirate peut aussi cumuler ces différentes techniques : téléphoner pour obtenir un rendez-vous puis confirmer par e-mail pour mieux vous gruger lors de l'entretien où vous vous rendez compte qu'il partage la même passion que vous pour la pêche à la mouche ! Pour une entreprise, il est absolument vital de former le personnel à ce genre de problème. Un pirate prend soin de s'attaquer aux personnes les plus «faibles» techniquement : secrétaires, comptables, stagiaires et les petits nouveaux.

Kevin Mitnick et son «Art of Deception»

Si vous souhaitez en savoir plus sur le social engineering, sachez que Kevin Mitnick a coécrit un livre entier sur ce sujet. Celui qu'on considère comme le meilleur hacker du monde n'a pas uniquement réussi grâce à ses talents en informatique. «L'art de la supercherie» («The Art of Deception»), publié en 2002 traite de l'art du social engineering principalement par le biais de la téléphonie. Si vous êtes plutôt «cinéma», vous trouverez quelques exemples dans le film retraçant une partie de la vie de Mitnick : Cybertr@que (Takedown).

Controlling the Human Element of Security

THE ART OF
DECEPTION

KEVIN D. MITNICK



Ils fabriquent de la DROGUE !

C'est bien connu, on trouve de tout sur Internet ! Avant que la police du Net apprenne à se servir d'un mulot, on trouvait même des sites qui proposaient toutes sortes de drogues en vente par correspondance. Mais maintenant que le réseau des réseaux est sous étroite surveillance, les cyber-dealers sont de plus en plus rares. La nouvelle mode est aux sites de «recettes» : héroïne, LSD, oxycodone, GHB, cocaïne, etc.

QUID DE LA LOI ?

La production et/ou la fabrication illicites de stupéfiants sont un crime, passible de 20 ans de réclusion criminelle et d'une amende de 7 500 000. Cette peine pouvant être portée à 30 ans si les faits sont commis en bande organisée. De quoi refroidir les apprentis botanistes/chimistes.

i

Le phénomène est tellement «à la mode» qu'une série a vu le jour. Breaking Bad ou l'histoire d'un prof de chimie qui se met à fabriquer de la méthamphétamine pour subvenir aux besoins de sa famille



Les sites proposant des graines de cannabis et les moyens de cultiver de chez soi ne manquent pas sur la Toile. On en trouve même proposant le matériel adéquat pour commencer ce type de culture dans un simple placard. Évidemment puni par la loi, ce type de pratique n'a cependant jamais tué personne. Par contre, on trouve de plus en plus de sites qui proposent des protocoles très détaillés permettant de faire à la maison des drogues beaucoup plus puissantes. Notre confrère Zataz.com a dernièrement fait état d'un site qui proposait des livres entiers sur le sujet pour un abonnement d'une vingtaine d'euros mais avec un peu de persévérance, nous avons trouvé des sites qui proposaient gratuitement de telles informations. Et les réseaux P2P ne sont pas en reste...

Papa est en haut, il fait de l'héro...

Attention, il n'est pas si facile de réaliser de telles drogues chez soi avec du matériel volé en cours de chimie. Mais comme les sommes en jeu sont considérables, l'investissement est payant. Pourtant, des apprentis chimistes commencent à se faire attraper par la police. L'année dernière, un jeune homme habitant Bourgoin-Jallieu a commandé sur Internet 900 g de feuille de coca et un litre

d'huile de sassafras pour faire ses propres comprimés d'ecstasy. Il a expliqué à la police qu'il était simplement entré en contact avec un administrateur de forum qui lui avait expliqué comment réaliser sa «popote» et où trouver les «ingrédients». L'apprenti Escobar ne savait pas que l'huile de sassafras, à la fois utilisée dans la parfumerie mais aussi comme médicament est bien connu des services de police pour être un précurseur de l'ecstasy. Cette huile essentielle est d'ailleurs interdite en France depuis 2007 et son importation est étroitement surveillée. Lors de la perquisition les policiers ont découvert un

véritable laboratoire... C'est d'ailleurs là tout le problème : l'appât du gain attire de plus en plus de gens vers ce genre dérive. Il faut pourtant savoir que la drogue de synthèse demande beaucoup de rigueur scientifique à produire. Comme toute manipulation chimique, le danger est grand et les risques sont multiples : explosion, contamination par des produits volatils, mauvais dosage entraînant un empoisonnement ou la mort. Même un élève studieux avec 20/20 en chimie et équipé du matériel adéquat (on parle ici de milliers d'euros d'appareil) n'est pas à l'abri d'une surprise qui peut être fatale...

Les herbes type «Legal buds» bannies de France

On trouve aussi sur Internet des sites qui vendent des alternatives à la marijuana : les Legal Buds. Présentées comme des herbes à parfumer ou comme de l'encens, elles ont été récemment interdites par le Ministère de la Santé et des Sports français (et ne sont donc plus «Legal»). Sans THC (la substance active du cannabis), ces mélanges d'herbe censés contenir de la queue de lion (un proche parent du cannabis) ou de la salvia divinorum (appelé sauge des druides) contiennent des molécules chimiques comme la CP47 ou la CP497, des cannabinoïdes très puissants réalisés en laboratoire. Il y a encore peu de temps, il suffisait de commander ces «herbes» pour les recevoir chez soi dans des petits paquets flashy avec des noms exotiques : Gorilla, Gold Spirit, Green Viper, etc. Voici un petit reportage très intéressant sur ce sujet diffusé sur TF1 : www.wat.tv/video/droque-sur-internet-1ap6n_2fv7_.html

Téléphone GSM :

ON VOUS flique ?

En une quinzaine d'années, le téléphone GSM est partout. On en compte maintenant presque autant que d'individus sur terre. Rien n'est donc plus tentant que d'utiliser cette technologie pour suivre les utilisateurs pas à pas ou espionner des conversations. Entre mythe et réalité...



Sur Internet, on trouve un peu de tout et de n'importe quoi concernant la possibilité de traquer un GSM. Il faut dire que la possibilité de localiser un individu sans bouger de chez soi est un véritable fantasme pour certaines personnes. Du coup certains sites en profitent pour faire des blagues (vous rentrez le numéro et vous vous retrouvez avec des photos de mauvais goût) ou pour arnaquer les plus crédules...

Où es-tu ?

Il est techniquement possible de localiser un téléphone GSM grâce à un procédé utilisé par la police : la triangulation. Il s'agit de calculer l'intensité de réception d'un signal à partir des 3 antennes relais les plus proches. Un peu comme dans les films, il est possible d'avoir une précision suffisante pour appréhender un suspect. Attention, il faut que le téléphone soit allumé dans une zone de réception suffisante. Plus fort, les téléphones plus récents qui sont équipés d'une puce GPS peuvent être localisés avec encore plus de précision. Il suffit pour cela que notre individu se connecte à son service GPS (ou une page Internet qui utilise le GPS) pour savoir avec une précision extrême. Mais si la police réussit ce tour de passe-passe, les citoyens peuvent-ils les imiter ? À moins de passer par un service spécial payant qui demandera l'accord au propriétaire du téléphone pour le localiser, il est impossible de faire quoique ce soit. Le service Ootay (www.ootay.fr) propose par exemple de géolocaliser les GSM de vos proches pour éviter l'absentéisme scolaire ou évitez le vol de votre téléphone. Une fois inscrit, il faut que le fournisseur accepte de géolocaliser la personne (car bien sûr, il n'est possible de suivre à la trace qu'un utilisateur

OOTAY® Vous cherchez les personnes qui vous sont chères ?

PROCHES-VOUS Sachez où sont les personnes qui vous sont chères...

La localisation ?
Histoires d'emploi
La sécurité
Envoyer à un ami

Perte de votre téléphone portable vous inquiète...

Le service OOTAY® vous aide à retrouver votre téléphone portable perdu ou volé.

4€ / mois
15€ / mois

Le service OOTAY® respecte la directive européenne 2002/58/CE ainsi que les recommandations de la CNIL en matière de protection de la vie privée.

Ootay, un des nombreux services qui permettent de traquer un GSM légalement



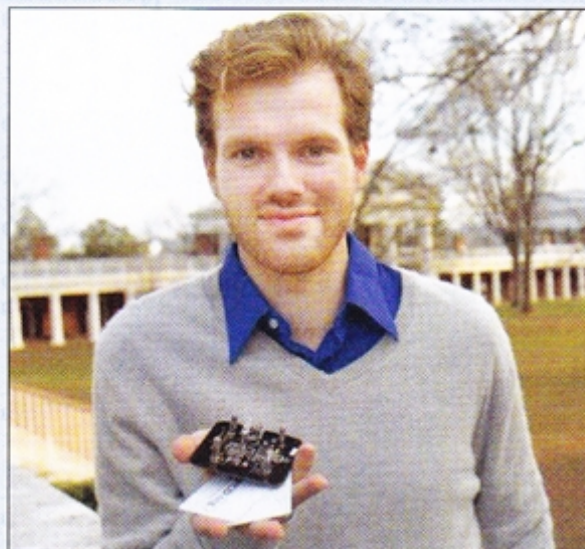
qui soit d'accord : enfants, amis, parents âgés, etc.) et que la personne que vous voulez localiser accepte les termes du contrat via SMS. Il suffit ensuite d'aller sur le site Internet du service ou sur le service WAP de Ootay puis lancer la géolocalisation. La personne est prévenue par SMS que vous venez de la retrouver mais il est un peu tard pour courir au lycée...

Les conversations bientôt hackées ?

En ce qui concerne les écoutes téléphoniques, la glace comment à se briser sous les pieds de la méthode de chiffrement A5/1. Le Chaos Computer Club (CCC), une des associations de hackers les plus influentes dans le monde promet même un contournement très rapide de cet algorithme. C'est d'autant plus inquiétant que de plus en plus de services demandant une sécurité optimale (banque mobile, etc.) commencent à se populariser sur ce réseau. La volonté du CCC n'est pas de jouer le jeu des organisations mafieuses mais surtout d'alerter le grand public et l'industrie téléphonique sur les risques qu'ils font encourir à leurs clients. Déjà l'année dernière lors d'une conférence au Pays-Bas,

une équipe de hackers a présenté une tentative d'attaque de l'algorithme A5/1. Cette dernière utilisait un «sniffer» (un appareil d'écoute qui n'enregistre que les conversations «cryptées») et un module d'analyse qui déchiffrerait la conversation. Le but étant de prouver la faiblesse de l'algorithme, ce projet Open Source ne prévoit pas un décryptage à la volée mais la technique est là...

Le responsable, Karsten Nohl, souhaite donc mettre les pieds dans le plat. Il estime actuellement à trois mois la durée totale qui serait nécessaire à ce que quatre-vingts ordinateurs, présentant de fortes capacités de calcul, puissent réaliser une attaque par force brute sur l'algorithme A5/1. Une fois cassé, l'algorithme permettrait de générer des tables pouvant être ensuite utilisées par tout un chacun. Au final, avec un ordinateur, l'équipement radio (le sniffer) et ces fameuses tables, il serait possible d'intercepter des conversations. Ce la vous semble énorme ? Sachez que l'algorithme A5/2 utilisé aux



Karsten Nohl estime que le protocole A5/1 est en bout de course...

États-Unis est plus faible encore que son homologue Européen... Pour la GSMA (l'association en charge du protocole GSM), Karsten Nohl sous-estime certains éléments du A5/1 notamment la partie concernant le ciblage et l'identification d'un appel GSM visé. L'association souligne aussi que son dernier rejeton, le A5/3, est progressivement mis en place et qu'il pourrait prendre la relève aussi bien sur la 3G que sur le GSM. Encore une fois, il s'agit d'une course de fond...

Quand le piratage se démocratise...

Pas forcément besoin d'attendre le prochain crack du A5/1 pour espionner des GSM ! De plus en plus de sites proposent des modifications de téléphones portables permettant d'espionner vos proches. Il suffit d'installer un programme sur un téléphone cible pour pouvoir écouter les conversations sans éveiller les soupçons. La liste des téléphones compatibles est de plus en plus longue. Plus fort : il est même possible d'offrir un portable déjà équipé ! Un autre pack évoque la possibilité d'espionner l'environnement du portable cible : un véritable micro activable à distance ! Tout est possible : enregistrement



via la caméra, enregistrement de la conversation lorsque vous ne pouvez pas surveiller, scan des SMS, MMS, interception des communications à la volée, etc. Il faut bien sûr avoir accès au téléphone de l'individu que vous voulez espionner mais cette activité est en pleine expansion. La cible est large : femmes ou maris trompés, espionnage industriel, espionnage de nourrice, surveillance

d'ado difficile ou simple curiosité. Attention, ce genre de site ne prévient pas toujours que ce type d'utilisation (comme le fait d'installer un programme sur le téléphone d'un tiers à son insu pour l'espionner) est complètement illégal en France...



Piratage de bases de données : Les nouvelles armes des hackers

Des pirates informatiques iraniens ont inventé un logiciel qui ne laisse aucune chance aux serveurs Internet. En quelques clics de souris, nous avons pu nous rendre compte que les données privées et sensibles sauvegardées sur les serveurs d'entreprises Françaises et étrangères étaient accessibles aux flibustiers du Web. Enquête !

Tout débute à la fin du mois de mai dernier. Un hacker français contacte la rédaction pour nous expliquer que certaines données de notre serveur Internet pouvaient être lues et copiées très simplement. «Il me suffit de quelques clics de souris pour accéder à l'ensemble des adresses électroniques de la rédaction» soulignait-il alors. Et effectivement, en quelques secondes, une base de données s'ouvrait à nos regards étonnés. Un tour de passe-passe digne d'un David Copperfield de l'informatique. Inquiétant ! Si notre hacker s'est donné pour mission de nous aider, nous allons découvrir que le business des bases de données sur Internet est devenu un gagne-pain fructueux pour des centaines de pirates informatiques. Des e-voleurs équipés de logiciels étonnants. De véritables passe-partout électroniques à l'image du logiciel X'j3v (Le nom a été modifié pour ne pas permettre aux scripts kiddies de s'en donner à cœur joie, NDLR), un programme créé par des bidouilleurs iraniens.

Petit outil, grands secrets

X'j3v ne paie pas de mine. Quelques boutons en anglais ; deux/trois

onglets ; aucun mode d'emploi. Pourtant, derrière ces quelques bits, une arme redoutable qui devrait permettre aux responsables informatiques de réfléchir à deux fois sur la sécurité de leurs serveurs. Dans le cas de cet «outil», il en existerait plusieurs dizaines du même type sur la toile, il suffit de rentrer une adresse Internet trouvée via le moteur de recherche Google. «Le plus terrible, souligne François (un pseudonyme), un pirate informatique, Il suffit de quelques mots clés dans Google pour établir le lien qui ouvrira les portes du site que je cible». Bilan de cette opération banale, le logiciel informatique se charge de trouver le point d'entrée à la base de données de n'importe quel site Internet. Opération que ce software effectue en moins de trois secondes. Vous avez bien lu, n'importe quel site Internet équipé d'une base de données est en danger. Lors de notre rencontre avec François, aux hasards de nos questions, l'intrus a été capable de nous présenter des serveurs faillibles appartenant à Orange, Paris Match, M6, mais aussi des sites gouvernementaux, des boutiques, des hôtels, ... «J'aurai pu effectuer

une razzia sur leurs informations, en quelques minutes» s'amusa alors notre interlocuteur. Dans sa démonstration particulièrement inquiétante, des données bancaires se sont affichées dans certains cas ; des identifiants de connexion ; les messages internes. Bref, l'ensemble des petits et grands secrets inscrits et sauvegardés dans la moindre base de données. À noter que François nous a fourni les liens et les accès fautifs afin que les sites découverts lors de notre entretien soient alertés et corrigés. Du remords le jeune homme ? Peut-être ! En attendant, lors de sa démonstration, nous avons pu voir défiler devant nos yeux écarquillés des dizaines de mots de passe, non chiffrés ; des données bancaires sauvegardées dans des bases de données de boutiques en ligne.

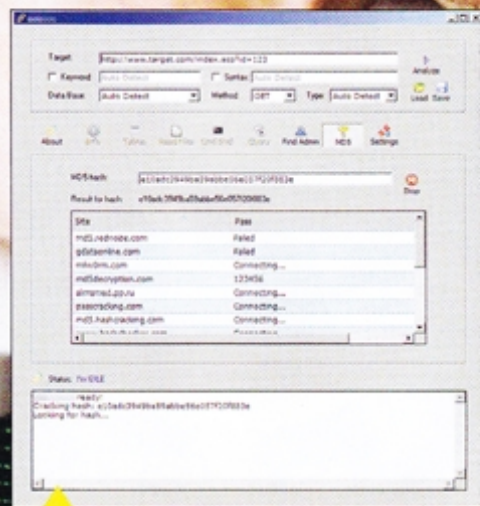
Une demande très forte pour ce type de données

Vicieux, l'outil décortique une par une les tables d'enregistrements sauvegardées dans les bases de données. En quelques secondes, selon les configurations des sites et serveurs Web, les identités, les adresses physiques, les courriels, les



Un marché noir en pleine expansion

Jérôme Granger, responsable de la communication de l'éditeur de solutions de sécurité informatique G DATA « Cette économie souterraine qui prend de l'ampleur. Le développement de l'économie souterraine au cours des dernières années s'illustre par le biais d'un exemple : Là où les pirates informatiques se vantaient autrefois d'arriver à obtenir via des données volées un accès gratuit à d'innombrables offres de pornographie sur Internet, ils se targuent aujourd'hui du nombre de cartes de crédit qu'ils ont déjà réussi à dérober. Fait remarquable : ces données se transforment à présent en espèces sonnantes et trébuchantes. Une tendance qui a fait naître une économie souterraine. Aujourd'hui, tout ce qui existe déjà dans un vrai environnement économique légal : fabricants, commerçants, prestataires de services et clients se trouve dans



l'économie des cyberdélinquants». Bref, le «black market» informatique a encore de beaux jours devant lui ! Pour rappel, tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physique (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de cinq ans d'emprisonnement et de 300 000 € d'amende (art. 226-17 du code pénal).



LIBRE ET ENGAGÉ

CR-ROM OFFERT !

Juillet / Septembre 2010

PEER 2 PEER
**CLICK P2P
LOAD P2P**

3^{'90}
€
PRIX CANON

LE GUIDE 100% PRATIQUE

MONTAGE VIDÉO

- DU CAMÉSCOPE AU PC
- CAS PRATIQUE :
UN MONTAGE DE PRO
AVEC MOVIE MAKER
- PARTAGEZ ET DIFFUSEZ
VOTRE FILM !

RETOUCHE PHOTO

- LES MEILLEURS SOFTS
ET SERVICES GRATUITS !
- PICASA : LE GUIDE COMPLET !
- CLASSEZ, ARCHIVEZ
ET PARTAGEZ VOS PHOTOS



Le **TOP 15** des
services en ligne
GRATUITS

PARTAGEZ VOS FILMS ET PHOTOS SUR INTERNET



+ CD OFFERT !



VOTRE MAGAZINE Nouvelle Génération

WikiLeaks :

un trublion impossible à mater



WikiLeaks est un site qui fait peur, même au gouvernement américain. Il s'agit d'une sorte de portail recensant des milliers de documents confidentiels qui n'auraient jamais dû sortir de là où ils étaient soigneusement rangés. S'ils sont arrivés en ligne, c'est grâce au courage de sources qui peuvent et doivent rester anonymes. Comment tout cela fonctionne-t-il ?

Lancé en 2007, WikiLeaks est un site permettant à tout à chacun de poster des «fuites» («leaks» en anglais). Qu'ils viennent des USA, de l'ex-URSS, de la Chine ou de pays africains, ces personnes prennent le risque de divulguer des informations qui sont en leur possession. Pour permettre leur protection, les échanges avec le site sont bien sûr sécurisés grâce au protocole SSL mais il est aussi possible d'utiliser le réseau TOR en sus pour plus de sûreté. L'envoi des informations passe par un simple formulaire. Il suffit de cliquer sur «Submit documents» sur la page de garde pour y avoir accès. Pour ne pas mettre en danger des personnes (notamment en ce qui concerne l'aspect militaire), il est aussi possible de mettre une date à laquelle le site pourra mettre la fuite en ligne. En plus de cette protection informatique, WikiLeaks offre aussi une protection légale et éthique. Les serveurs, basés en Suède et en

Belgique dépendent des lois de ces pays. Ces dernières sont en effet parmi les plus sûres du monde en ce qui concerne l'aspect de la protection des sources. Après tout, si une seule de ces personnes est inquiétée, c'est tout le système qui serait mis en danger...

WikiLeaks, une cible potentielle

Seulement voilà, pour certains gouvernements toute information n'est pas bonne à dire, surtout lorsqu'il s'agit de guerre et de vies humaines... Le 15 mars 2010, un document classé de 32 pages publié sur WikiLeaks montrait que les services secrets US cherchaient à détruire WikiLeaks en le marginalisant aux yeux du monde. Le rapport recommande «l'identification, la poursuite judiciaire contre les personnes, qui ont révélé au public des informations internes» via WikiLeaks. Deux ans après la date du rapport, aucune source n'avait été exposée... Le conditionnel est de rigueur puisque Bradley



Il faut sauver le soldat Manning !

Manning, un analyste du renseignement, a récemment été inculpé de douze chefs d'inculpation. Ce soldat de 22 ans est en effet soupçonné d'avoir remis au site la vidéo d'une bavure de l'armée américaine en Irak en 2007 (voir notre encadré). Seulement ici, WikiLeaks n'est pas responsable et si le jeune Manning est dans de beaux draps, c'est qu'il a été trop bavard et a été dénoncé. Accusé aussi d'avoir mis à disposition les «Afghan War Diary», Manning risque plus de 50 ans de prison... Julian Assange, le médiatique porte-parole de WikiLeaks, a quant à lui démenti que l'analyste soit sa source. Bien essayé Julian !

LES 3 PLUS GROS «COUPS» DE WIKILEAKS

1. Divulgateur d'une vidéo classée secrète (la fameuse «Collateral Murder») qui montre comment



18 personnes innocentes ainsi que 2 journalistes de Reuters ont été tués par un hélicoptère Apache durant une opération en Irak en 2007.

http://wikileaks.org/wiki/Collateral_Murder_5_Apr_2010

2. La mise en ligne du «Afghan War Diary» où plus de 91 000 documents classés reportent les innombrables difficultés de l'armée américaine dans ce pays : corruption des agents locaux, complicités du Pakistan, armement grandissant des Talibans, etc.

http://wikileaks.org/wiki/Afghan_War_Diary_2004-2010

3. La mise à disposition de documents très compromettants concernant le pillage des ressources du Kenya pendant la présidence Moi. Du comment grâce à des paradis fiscaux, des hommes de pailles et la complicité de nombreux autres pays, la famille de l'ancien Président a réussi à voler plus de 2 milliards de dollars aux Kenyans.

www.guardian.co.uk/world/2007/aug/31/kenya.topstories3



Sécurisez votre clé USB

Les menaces pesant sur votre clé USB sont nombreuses, vol de données confidentielles ou contamination due à un virus sur une machine tiers. Apprenez à protéger vos clés de manière efficace.

Attention ! Si votre clé USB est devenue votre meilleure amie, elle n'en reste pas moins fragile. De nombreuses menaces pèsent effectivement sur elle et, par conséquent, sur vous. Aussi pratiques que les disquettes, capables de contenir des gigas de données, plus rapides à copier que des DVD, les clés USB n'ont aucun défaut. Enfin presque.

Protéger ses données

Les appareils USB impliquent plusieurs risques sécuritaires. Des programmes, comme le tristement célèbre USB Dumper, s'attaquent à l'intégrité des informations transportées. Ce programme permet de copier

l'intégralité d'une clé sur l'ordinateur « hôte » sans que l'utilisateur ne s'aperçoive de rien. Face à de telles menaces, il n'existe pas dix mille solutions. Il faut crypter les données sensibles. Nous avons tous sur nos ordinateurs des données auxquelles nous tenons particulièrement : images, films, musiques mais aussi mots de passe, projets professionnels ou carnets d'adresses. Le logiciel TrueCrypt est capable de chiffrer ces informations « à la volée ». Son seul défaut, c'est qu'il nécessite d'être aussi installé pour décrypter les fichiers. Heureusement, il existe une astuce pour l'installer sur votre clé USB.

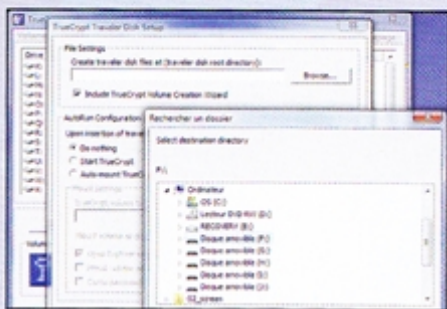
Se protéger contre les virus

La perte de données confidentielles n'est cependant pas le seul danger que vous devrez affronter avec votre clé. Les appareils USB, en général, sont les cibles privilégiées des attaques de virus. Ceux-ci se transmettent, de manière transparente, de clés en ordinateurs et réciproquement. Le soft gratuit Dr Web permet de protéger efficacement sa clé, mais il vous demandera sans cesse une mise à jour vers la version payante. L'autre solution consiste à installer Clamwin Free Antivirus, logiciel libre, dont le seul défaut est de ne pas faire de protection résidente.

Protégez vos données

1 INSTALLER TRUECRYPT SUR VOTRE CLÉ

Commencez par télécharger le logiciel (www.truecrypt.org) et installez-le sur votre ordinateur. Ensuite, dans le menu **Tools**, choisissez **Traveler Disk Setup**. Parcourez votre ordinateur et sélectionnez votre clé. Laissez l'option suivante sur **Do nothing**. Cliquez sur **Ok**, puis **Create**. Votre clé USB contient à présent un dossier **TrueCrypt**.

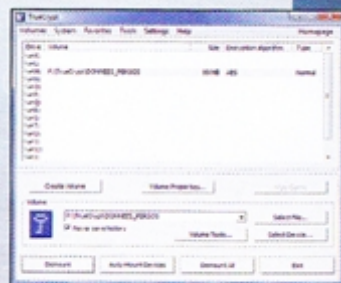


2 ICRÉER UN VOLUME

Double-cliquez sur **TrueCrypt-Format.exe** et sélectionnez la première option, **Create an encrypted file container** ou, si vous souhaitez utiliser toute la clé USB comme conteneur crypté, cochez **Encrypt the entire system drive**. Choisissez ensuite **Standard TrueCrypt Volume**. Dans le panneau **Volume Location**, créez un nouveau fichier d'encryptage, nommez-le, par exemple, **DONNEES_PERSOS**. Il sera situé sur votre clé, dans le dossier **TrueCrypt**. Il ne vous reste plus qu'à paramétrer l'encryptage. Les algorithmes **AES** et **RIPEMD-160** constituent une combinaison relativement inviolable. Entrez l'espace que vous souhaitez allouer à vos fichiers protégés et créez votre mot de passe. Cliquez enfin sur **Next** pour lancer le formatage de votre clé.

3 IPROTÉGEZ VOS DOCUMENTS

Votre volume est maintenant prêt à être utilisé et à recevoir vos fichiers sensibles. Double-cliquez sur le fichier **TrueCrypt.exe** se trouvant sur votre clé USB. Cliquez sur **Select File** et allez chercher le fichier **DONNEES_PERSOS**, cliquez sur **Mount** et entrez votre mot de passe. Magique, votre clé apparaît sur le disque virtuel que vous venez de sélectionner. Ce disque se trouve maintenant dans votre explorateur. Utilisez-le comme un disque classique. Après vos opérations, cliquez sur le bouton **Dismount** et débranchez votre clé USB.





Blindez votre FaceBook !

La société Reputation Defender a récemment mis au point une application FaceBook, permettant de sécuriser sa page. Dotée d'une interface visuelle conviviale, l'application Privacy Defender règle automatiquement vos paramètres pour que rien ne filtre.

Pirate ou pas, vous utilisez certainement FaceBook, ne serait-ce qu'à titre « consultatif ». Si vous vous êtes pris au jeu, vous ne souhaitez sans doute pas que vos photos de soirée ou votre numéro de téléphone ne tombent entre n'importe quelles mains. Notamment celles des publicitaires, qui on3t fait de FaceBook leurs choux gras. Imaginez-vous un jour de tomber nez à nez avec une photo de vous sur un panneau de quatre mètres de large ? Sans aller jusque-là, la politique de protection de la vie privée de FaceBook laisse à désirer et semble changer tous les quatre matins. Difficile de s'y retrouver entre toutes les options, malgré les récents efforts de transparence effectués par le plus grand réseau social au monde. Privacy Defender est une application simple d'utilisation, qui dresse, dans un premier temps, un état des lieux sur la sécurité de votre compte. Un graphique vous montre alors, les failles qui ont été détectées. Vous pouvez ensuite, en un seul clic, les régler ou les ignorer. Voilà donc une manière simple et efficace de laisser les photos de vos soirées les plus arrosées sur FaceBook, sans craindre de les voir apparaître là où vous les attendez les moins.

OÙ TROUVER PRIVACY DEFENDER

 www.privacydefender.net

 <http://apps.facebook.com/privacy-defender/>

Verrouillez votre compte FaceBook

1 SCANNEZ VOS DONNÉES

Connectez-vous à votre compte FaceBook et rendez-vous sur la page de l'application Privacy Defender (<http://apps.facebook.com/privacydefender/>). Cliquez ensuite sur le bouton **Autoriser**, pour permettre à Privacy Defender de scanner vos paramètres.



2 DRESSEZ LE BILAN

Une fenêtre apparaît et vous propose de rajouter le bouton Privacy Defender dans votre barre de favoris. Deux solutions s'offrent à vous, faites-la glisser avec la souris ou faites un clic droit et **Ajouter aux favoris**. Cliquez ensuite sur le bouton, l'analyse peut prendre quelques minutes. Le graphique suivant vous informe sur plusieurs niveaux de sécurité.



3 RÉPAREZ LES FUITES

Tous d'abord, Privacy Defender vous montre si les partenaires publicitaires de FaceBook ont accès à vos données publiques, si vos amis peuvent accéder à vos infos persos et enfin si les annonceurs peuvent montrer vos données à vos amis pour des publicités. Le camembert principal vous permet de régler tous ces détails au cas par cas. Cliquez sur les cases pour ajuster précisément ou utilisez le curseur tout en bas. Une fois que vous êtes satisfaits, cliquez sur le bouton **Fix My Privacy** ! Privacy Defender paramètrera automatiquement vos données. N'hésitez pas à organiser ce scan régulièrement, car les conditions d'utilisation de FaceBook changent souvent.



L'ART DE LA STÉGANOGRAPHIE

Pourquoi crypter des informations lorsque l'on peut les dissimuler ? Là où les « gros bras » chiffrent, les petits malins utilisent la stéganographie : un procédé très ancien qui consiste à cacher la vraie nature d'un document. Pour plus de sécurité il est même possible de combiner les deux !

Le but de la stéganographie est de dissimuler un message dans un autre document pour berner un éventuel petit curieux. Cette pratique est utilisée depuis l'Antiquité pour transmettre des informations sans éveiller les soupçons de l'ennemi. L'historien grec Hérodote raconte que pour inciter Aristagoras à se révolter contre Darius, Histée fit raser la tête d'un esclave, lui tatoua son message sur le crâne. Il attendit alors que les cheveux eussent repoussé puis envoya son esclave délivrer son message sans risque qu'il soit intercepté avec une lettre compromettante. Les encres sympathiques, utilisé dès le premier siècle avant Jésus Christ, constitue aussi un procédé stéganographique : l'acide citrique contenu dans

le citron a une température d'inflammation est plus basse que celle du papier. Chauffé, une réaction d'oxydation laissera apparaître le message sur le papier. Plus amusant, les messages d'amours à double sens entre les écrivains George Sand et Alfred de Musset que vous retrouverez à cette page : <http://5ko.free.fr/fr/sand.html>.

La magie du numérique !

À l'heure d'Internet et des échanges d'informations, la stéganographie a franchi un nouveau pallier. Il est possible de dissimuler des messages, des photos, des sons dans un autre document avec un simple logiciel. Il suffit pour cela de jouer avec les octets qui codent pour la couleur de la photo. La méthode la plus courante consiste à modifier les «

bits de poids faible » (ou « least significant bit » en anglais). Même modifiés, ces derniers n'altèrent que très peu le rendu final d'une photographie mais il s'agit d'une suite suffisamment conséquente de bits pour qu'elle puisse constituer un message. Dans la pratique, il est possible de cacher 130 Ko de texte dans une image de 250 Ko sans que celle-ci ne soit suspecte (il serait en effet bizarre de trouver une photo de très mauvaise qualité pesant plusieurs Mo). Outre les couleurs, il est possible de jouer sur la méthode de compression d'un document ou de dissimuler un message dans un fichier sonore. Dans ce cas, les bits de poids faible changeront de manière imperceptible le son pour une oreille humaine. Tout est possible à condition que l'émetteur

et le destinataire se soient entendus sur la méthode...

Dans la pratique

Imaginez Alice, citoyenne d'un pays totalitaire, souhaitant faire parvenir un message à Basile. Il suffit à Alice de dissimuler sa prose dans une image anodine qu'elle publiera dans son blog ou qu'elle enverra par email. Même surveillée,

Alice ne risque rien tant que la méthode de dissimulation n'est connue que d'elle et de Basile. C'est pour cela que la sténographie est particulièrement adaptée pour des dissidents ou pour des terroristes. Après les attentats du 11 septembre 2001, les services secrets américains ont d'ailleurs soupçonné Al Qaida de transmettre des directives en les cachant dans des images transitant

par Internet. Avec la quantité d'informations qui transitent, il faut d'abord savoir où chercher puis déjouer la malice de l'expéditeur. De surcroît, la sténographie peut aussi être ajoutée à un chiffrement. En effet rien n'empêche l'émetteur de crypter le message qu'il a dissimulé. Comment obtenir la clé ? En la dissimulant dans un autre document...

Dissimulez des documents avec Stegano

En France nous pouvons (encore) nous exprimer librement. Pour envoyer des messages originaux ou s'entraîner pour le jour du couronnement de Sarko ler, nous allons voir comment dissimuler un texte dans une image sans que celle-ci paraisse suspecte. Même si des logiciels comme Steganos (avec un « s ») ou Invisible Secrets sont très complets, nous allons utiliser Stegano qui lui est gratuit...

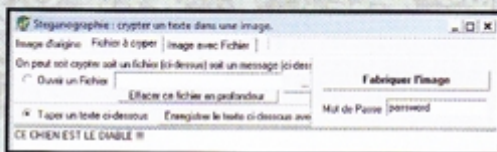
1 L'IMAGE D'ORIGINE

Tout d'abord, allez télécharger le logiciel à cette adresse : <http://www.mike-soft.fr/Softs/Stegano/Logiciel%20stegano.htm>. Une fois installé, démarrez-le puis dans l'onglet **Image d'origine** cliquez sur les trois petits points pour ouvrir l'image de votre choix. Dans notre exemple, cette image de chien pèse 2 359 296 octets. Le logiciel vous informe alors qu'il est possible d'y dissimuler un fichier ou un texte de 1 669 096 octets ! Notez que vous pouvez recadrer votre image à la souris directement dans le logiciel.



2 UN MOT DE PASSE ?

Dirigez-vous ensuite vers le deuxième onglet (**Fichier à crypter**). Ici vous avez le choix entre taper directement un texte ou choisir un fichier de votre disque dur. Il est tout à fait envisageable de placer une autre image à l'intérieur de la première... Pour plus de sécurité, le logiciel vous permet en plus d'ajouter un mot de passe. En effet, si un intercepteur connaît cette méthode de dissimulation (ici, le message est caché dans les octets qui codent les couleurs), il faudra en plus qu'il connaisse le mot de passe. Si vous habitez en Chine, nous vous conseillons d'être plus créatifs que nous concernant le mot de passe !



3 L'IMAGE FINALE

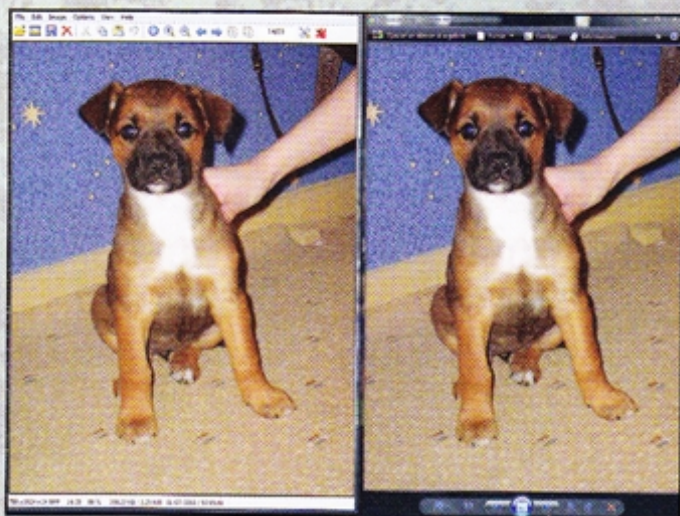
Cliquez enfin sur **Fabriquer l'image** pour faire apparaître votre image modifiée. Sélectionnez ensuite **Enregistrer l'image ci dessous avec ce nom** pour sauvegarder votre fichier sur le disque dur. Attention, celle-ci se nomme **Message** par

défaut, il faudra donc changer le nom car une image de chien qui porte le nom de « message » est plutôt suspecte, drôle de nom pour un chien non ? Notez que votre image finale est au format Bitmap (BMP) car ce type de fichier n'est pas compressé à l'inverse du JPEG. En effet une compression occasionnerait la perte pure et simple de votre message. Ne modifiez donc pas votre image si vous voulez que l'astuce fonctionne : recadrage, conversion ou retouche sont à proscrire !



4 LA RESTITUTION DU MESSAGE

Vous pouvez vous amuser à comparer l'image de départ et l'image modifiée mais les différences sont invisibles... Armé du même logiciel, le destinataire devra ouvrir l'image dans le troisième onglet, entrer le mot de passe et cliquer sur **Décrypter l'image**. Il retrouvera alors notre message caché : **CE CHIEN EST LE DIABLE !!!**



Modifier **votre voix** au **téléphone**

On peut se demander quel est l'intérêt de modifier sa voix pour un pirate. Pourtant cette technique se prête très bien au social engineering : un procédé qui permet de récupérer des informations sur des tiers ou des entreprises dans le but de les tromper ou d'obtenir des renseignements plus sensibles (voir notre article page 10).

Plus c'est gros et plus ça marche ! Nous avons vu page 10 qu'il était à la portée de tout le monde d'obtenir des renseignements confidentiels sur un tiers. Il suffit parfois d'un peu de bagou et d'une bonne dose de confiance en soi pour rouler le plus méfiant des quidams. Encore plus fort : avec un simple logiciel métamorphosant votre voix, il est possible d'améliorer votre technique. En plus de la voix, certains types de logiciels permettent aussi de simuler des bruits de fond

comme une salle de travail, etc. Vous recevez un coup de fil avec la voix d'une femme qui veut vous poser «quelques questions» sur vos habitudes de surf, de consommations, etc. La voix est sensuelle, la personne a beaucoup d'humour et vous entendez dans le fond d'autres conversations avec des bruits de téléphones. Pour vous pas de doute, cette belle jeune femme a un boulot bien ennuyeux et vous compatissez. Pour ne pas être désagréable vous acceptez de répondre à ses



questions. À début d'ordre général («Vous êtes plutôt yaourt au fruit ou nature ?»), les questions deviennent de plus en plus personnelles. Vous êtes tombé dans le piège.

Des informations pas si anodines...

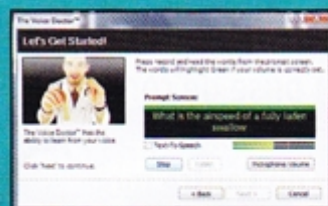
En moins de deux, vous avez donné le nom de jeune fille de votre mère, la marque de votre première voiture ou votre plat préféré. Cela ne vous rappelle rien ? Ce sont ces fameuses questions «de sécurité» qui permettent de retrouver ou de changer un mot de passe... Si en plus vous avez donné votre email, vous pouvez dire adieu à votre compte Paypal, votre compte mail (où se trouvent encore d'autres informations «sensibles»), etc. Bien sûr la personne que vous imaginiez s'appeler kévin92, elle n'est pas dans un centre d'appel à la recherche du prince charmant mais chez elle avec un logiciel de modulation de voix en train de vous rouler. Vous n'avez rien vu venir car tout a été réalisé pour vous faire croire à une histoire. On peut bien sûr imaginer d'autre situation avec des voix d'enfants ou de personnes âgées. Il est possible d'utiliser ce type de logiciel pour simplement faire une blague, pour prouver une discrimination ou pour rappeler une personne sans pour autant qu'elle vous reconnaisse. Le logiciel MorphVOX autorise ce genre de bidouillage. Ce dernier «apprend» votre voix et traite son signal en fonction de votre timbre ou de la gravité. Voyons comment l'utiliser et en tirer profit...

Changez votre voix avec MorphVOXPro

MorphVOXPro est un logiciel payant (32 €) que vous pouvez essayer pendant 7 jours. Ce logiciel est enrichi de centaines de voix et d'effets spéciaux (distorsion, bruits de fond). Vous pouvez transformer votre voix avec des filtres allant des plus graves aux plus aigus. Si vous voulez juste essayer le dispositif, sachez qu'une version gratuite (MorphVOXJunior) est aussi disponible mais elle propose bien moins d'options...

1 L'ANALYSE

Lorsque vous démarrerez MorphVOXPro celui-ci va tout d'abord charger un assistant qui va analyser votre voix. Cette étape est indispensable pour transformer le son au mieux des possibilités du logiciel. Il faut en effet que votre voix soit crédible... Si vous ne possédez pas de micro-casque, cliquez sur la case **Echo Cancellation** et validez. Paramétrez ensuite les périphériques d'entrée et de sortie (si vous n'avez qu'un seul casque ou micro, laissez tel quel). Rentrez ensuite un nom pour votre profil de voix et cliquez sur **Record** lorsqu'on vous le propose. Lisez alors la phrase qui s'affiche à l'écran. Cette dernière est en anglais mais même si vous avez un très mauvais accent, cela n'aura que peu d'incidence sur le résultat. Si le résultat est bon, la phrase deviendra verte. Sinon il faudra régler votre microphone ou le repositionner. Cliquez sur **Next** jusqu'à ce que l'assistant disparaisse.



2 LES VOIX

Vous arrivez alors à la fenêtre principale. Sur la gauche, vous pourrez choisir une voix de robot ou de démon mais celles qui nous intéressent sont celle de l'homme (vous masquez votre voix), celle de la femme (pour changer un peu ou «charmer») et celle du petit garçon (tout aussi efficace : «Allo madame, j'ai oublié le code pour rentrer»). Cliquez dans celle qui vous intéresse et parlez dans le micro. Miracle, votre voix est transformée ! Si vous n'êtes pas entièrement satisfait du résultat, il est possible de faire des réglages dans **Tweak Voice**. Ici vous pouvez changer le timbre ou la force de la voix. Lors d'un appel, il est aussi possible d'activer une option pour ne pas s'entendre (cliquez sur **Listen**) ou bidouiller l'équalizer (à droite). Les **Voice Effects** sont aussi à essayer... Si vous voulez ajouter des types de voix, sachez qu'il vous en coûtera quelques deniers (**Get More Voices**).



3 LES BRUITS DE FOND

En ce qui concerne les bruits de fonds, il faudra passer par les **Backgrounds**. Il n'existe malheureusement que deux options (les autres sont payantes) : la circulation avec les bruits de moteurs et les klaxons ou le centre commercial. À vous d'imaginer des situations pour l'une et l'autre («je suis bloquée dans les embouteillages, aidez-moi») ou «C'est le magasin X, où devaient-vous livrer au fait ?». Pour chaque bruit de fond il est possible de régler l'intensité. En ce qui concerne la mise en place de votre canular, sachez qu'il est possible d'utiliser ce logiciel avec Skype, MSN, etc. Pour un vrai coup de fil, il va falloir gruger et positionner le combiné en face de vos enceintes et se tenir suffisamment loin des deux pour ne pas dévoiler votre vraie voix. L'option **Echo Cancellation** est ici tout indiquée. Faites quelques essais avec des amis auparavant pour être sûr de votre petite supercherie.



Prenez le contrôle ... à distance !

La prise de contrôle à distance revêt bien des aspects. D'un côté nous avons les pirates qui essaieront de s'approprier le PC d'une personne par challenge ou pour obtenir des informations et de l'autre monsieur tout le monde qui désire aider un ami à distance ou avoir accès à des documents sans se déplacer. Voyons tout cela de plus près...

COMMENT SE PROTÉGER ?

1. Attention aux spams et aux emails vous invitant à découvrir un logiciel extraordinaire
2. Les sites de warez ou pornographiques peuvent abriter des malwares de ce type...
3. Ne laissez pas un inconnu se servir de votre PC et verrouillez la session lorsque vous vous absentez
4. Paramétrez correctement votre pare-feu Windows ou dotez-vous du firewall gratuit ZoneAlarm.

C'est l'angoisse de tout possesseur d'ordinateur : un beau matin vous ouvrez votre PC et le pointeur de votre souris n'en fait qu'à sa tête. Vous avez beau déconnecter Internet, le problème revient immédiatement dès que vous revenez sur le réseau. Vous êtes victime d'une prise de contrôle à distance ! L'intrusion peut être plus pernicieuse : vous ne remarquez rien mais un petit malin scrute l'intégralité de votre disque dur à la recherche de tout ce qui sera utile pour usurper votre identité, vous voler ou vous faire chanter... Libre à lui ensuite de formater votre ordinateur ou de transformer votre beau Dual Core en PC zombie qui ira rejoindre des milliers d'autres sur un botnet. En effet si votre PC ne comporte plus rien d'intéressant pour notre pirate, il pourra s'en servir pour attaquer d'autres ordinateurs ou l'utiliser pour lancer des attaques DoS contre des sites (de l'anglais «Denial of Service» : une



immense quantité de requêtes envoyées vers un site pour le faire saturer).

L'espion et le bon samaritain

De plus en plus difficile à mettre en place grâce à la démocratisation des firewall, une prise de contrôle à distance est pourtant toujours envisageable pour un pirate aguerri. Il est possible de se faire contaminer par e-mail ou en surfant sur un site douteux. Un clic au mauvais endroit et les ennuis commencent. Une fois contaminé par un malware de type Cheval de Troie (Trojan), ce dernier va affaiblir les défenses de votre PC et permettre la mise en place d'un logiciel de contrôle à distance. Sans que vous ne remarquiez rien (c'est d'ailleurs la condition sine qua none pour que le «travail» du pirate soit le plus discret possible), votre PC est en libre accès. On peut aussi imaginer qu'un individu installe un logiciel de contrôle à distance sur votre PC pendant votre absence. Une fois sur la machine, il saura exactement ce que vous faites bien au chaud chez lui. C'est pour cela qu'il faut absolument être prudent avec les personnes qui peuvent avoir accès à votre ordinateur. En dehors de ces techniques de pirate, vous aussi pouvez prendre contrôle d'un ordinateur à distance pour aider un ami, votre grand-mère ou pour ne pas vous déplacer à chaque fois que vous aurez besoin de consulter un document placé sur un autre PC. Dans notre pas à pas, nous vous présentons Crossloop, un logiciel très simple et qui permet de faire tout cela et même plus...

Prenez le contrôle avec Crossloop



CrossLoop est un outil de partage d'écran conçu pour permettre à des utilisateurs non techniques de se connecter à un PC distant en quelques secondes. Disponible en français, la version gratuite ne permet que de se connecter à un seul PC à la fois. C'est bien assez pour aider un ami un peu «noob» ou pour consulter des documents sur l'ordinateur du bureau...

1

ON NE PEUT PLUS SIMPLE

Pour utiliser Croolooop, dirigez-vous à cette adresse (www.crossloop.com) et créez-vous un compte gratuitement. Après avoir validé votre compte (regardez votre boîte aux lettres), téléchargez et installez-le logiciel. Bonne surprise, vous n'avez pas à bidouiller votre firewall...



2

LE PARTAGE

Crossloop ne comporte que deux onglets. **Partage** indique le nom de votre PC et le code d'accès que vous donnerez à la personne qui voudra avoir accès à votre PC (par téléphone, e-mail ou messagerie instantanée). À l'inverse, **Accès** permet de trouver un PC distant : vous n'avez qu'à rentrer le code d'accès et à cliquer sur Connexion pour vous y rendre...



3

QUELQUES PRÉCISIONS...

Attention, vous ne pourrez pas utiliser ce logiciel à des fins peu recommandable puisque l'ordinateur distant est toujours informé par une fenêtre quand l'ordinateur «maître» est sur le point de prendre le contrôle. Lorsque le maître prend les commandes, la souris et le clavier du PC est distant sont désactivés cependant ce dernier peut couper la connexion quand il veut...



AVEC XP ET VISTA

Il est tout à fait possible de prendre le contrôle d'une machine sans pour autant installer de logiciel. Il faut pourtant que ce PC soit équipé de Windows XP Pro, de Vista Intégrale ou de Windows 7. Avant toute chose il faut savoir que sur Internet, toute machine connectée est repérée par une adresse IP. Malheureusement, les internautes n'ont souvent que des IP dynamiques qui varient à chaque fois que vous vous connectez (et même parfois complètement aléatoirement dans la journée). Pour ne pas être embêté lorsque vous voulez vous connecter à un PC (pas facile de connaître l'IP

à distance !), il existe la solution www.DynDSN.org : un service qui vous attribue gratuitement un nom de domaine et qui suit à la trace les évolutions de votre IP dynamique... Ensuite, sous Windows XP Pro, faites un clic droit dans **Poste de Travail** et choisissez **Propriétés**. Activez ensuite l'onglet **Utilisation à distance** et cochez la case **Autoriser les utilisateurs à se connecter à distance**. Ensuite, à distance, il suffit de lancer le programme **Connexion bureau à distance** dans les accessoires de communication et de saisir l'adresse IP (ou l'URL si vous utilisez DynDSN) du PC cible. Pour Vista



Intégrale, il faut aller dans le menu **Démarrer** puis faire un clic droit sur **Ordinateur**. Ici, choisissez **Propriétés** > **Paramètres systèmes avancés** > **Utilisation à distance**. Dans **Bureau à distance**, cochez la case **Autoriser la connexion des ordinateurs...** puis validez.



LES

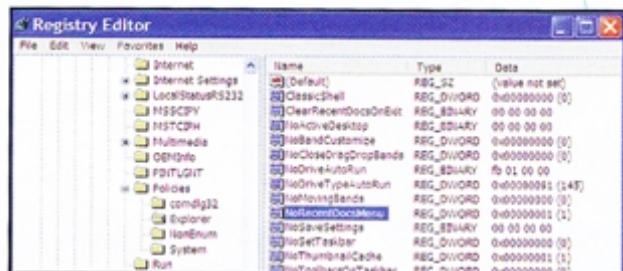
ASTUCES

DE LA RÉDACTION

Masquer une partition avec Windows

Si vous avez l'envie ou le besoin de masquer une partition ou un disque dur de votre système, il existe une solution pour Windows XP, Vista et 7.

Cliquez sur le bouton **Démarrer** et choisissez la commande **Exécuter**. Dans la fenêtre qui apparaît, tapez **regedit** et validez en cliquant sur le bouton **OK**. Pour



Vista et 7, tapez juste **regedit** dans le champ **Rechercher** du menu **Démarrer**. Repérez dans l'arborescence, la clé **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** et double-cliquez dessus. Créez une nouvelle valeur **Dword** nommée **NoDrives** en cliquant avec le bouton droit de la souris dans la zone droite de la fenêtre, puis en sélectionnant les commandes **Nouveau** et **Valeur Dword**. Affectez à cette chaîne une des valeurs suivantes en fonction du lecteur que vous désirez cacher :

Masquer le lecteur A : 1
Masquer le lecteur B : 2
Masquer le lecteur C : 4 (à éviter !)
Masquer le lecteur D : 8
Masquer le lecteur E : 16
Masquer le lecteur F : 32
Masquer le lecteur G : 64
etc.

Vous pouvez cacher plusieurs lecteurs, dans ce cas, additionnez tout simplement les valeurs : Pour cacher le lecteur A et le lecteur C, saisissez 5. Fermez l'éditeur de base de registres et redémarrez...

Retrouvez un mot de passe ZIP avec ZIP Password Finder

Vous avez sans doute déjà remarqué que certains fichiers ZIP peuvent être protégés par des mots de passe. Très pratique pour éviter qu'un individu n'accède à vos dossiers, ces mots de passe sont pourtant faciles à oublier ! ZIP Password Finder permet de



retrouver le mot de passe d'une archive au format ZIP en "brute force". Il s'agit en fait d'essayer tous les mots de passe possible afin de retrouver le bon. Pour réduire le champ de recherche, il est possible de spécifier le nombre ou le type de caractères (chiffres, minuscules, majuscules, ASCII, etc.) Le logiciel indique le temps estimé pour avoir un aperçu du niveau de sécurité du mot de passe (c'est d'ailleurs aussi un bon moyen de les tester)...



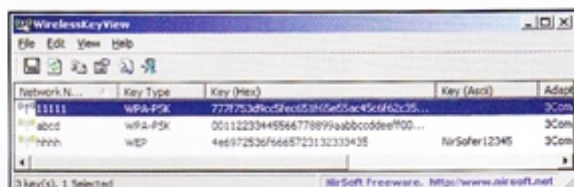
www.astonsoft.com

Disque de remise à zéro avec Windows Vista

Windows Vista (mais aussi Windows 7) dispose d'une option permettant de créer un "disque de remise à zéro". Il s'agit en fait de réinitialiser vos mots de passe de connexion dans le cas où vous les oublieriez. Cette sauvegarde, qui ne pèse qu'une poignée de Ko, ira se loger dans une vieille clé USB par exemple. Insérez votre clé USB obsolète dans un des ports libres du PC et attendez que le système la reconnaisse. Cliquez alors sur **Démarrer**, allez dans le **Panneau de configuration** et cliquez sur **Comptes d'utilisateurs**. Dans le panneau de gauche, tout en haut, cliquez sur **Créer un disque de réinitialisation de mot de passe**. Sélectionnez alors la lettre correspondant à votre clé et entrez le mot de passe du compte actuel. Cliquez sur **Suivant** puis sur **Terminer**. Retirez la clé USB et mettez-la dans un endroit sûr. Le jour où vous n'arriverez plus à vous connecter sous Vista, réinsérez la clé USB créée ci-dessus, cliquez sur le lien **Réinitialisez le mot de passe** (il apparaîtra dès le premier échec) et suivez l'assistant...



Retrouvez votre mot de passe Wi-Fi avec WirelessKeyView

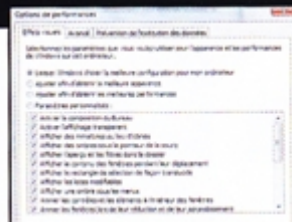


S'il vous est impossible de vous souvenir de la clé de l'un de vos réseaux Wi-Fi, pas besoin de retourner l'appartement ou de réinitialiser votre routeur ! Il suffit de faire confiance à l'utilitaire WirelessKeyView. Installez le logiciel sur le PC que vous utilisez généralement pour vous connecter à votre réseau et il vous dévoilera les clés de tous les réseaux sans fil enregistrés par Windows dans un champ baptisé **Key (Hex)**.

 www.nirsoft.net

Protection contre les malwares avec Windows

Pour s'immiscer dans votre système, les pirates utilisent des failles logicielles pour glisser des malwares au cœur des applications en cours d'exécution. Or depuis la version SP2 de Windows XP, il est possible d'activer le DEP (Data Execution Prevention) pour surveiller d'un peu plus près les services, DLL, programmes ainsi que contrôler la mémoire. Même si ce mode DEP est activé d'office avec les programmes et services intégrés à Windows (Explorer, etc.), il faudra le faire manuellement avec les autres. Ouvrez le **Panneau de configuration** de Windows, vérifiez que vous êtes bien en mode **Page d'accueil** et cliquez sur **Système et maintenance**. Cliquez ensuite sur **Système** puis sur **Paramètres système avancés**. Acceptez l'élévation de privilèges, cliquez sur le bouton **Paramètres** de la section **Performances** puis ouvrez l'onglet **Prévention de l'exécution des données**. Enfin, cochez la case **Activer la prévention d'exécution des données pour tous les programmes...** Si certains programmes rencontrent des plantages via ce mode, cliquez sur **Ajouter** puis sélectionnez-le pour l'ajouter à la liste des exceptions. Validez et redémarrez le système.



Protégez votre vie privée avec l'iPad

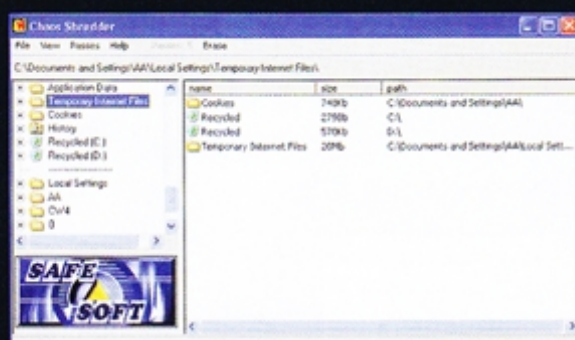


C'est joli un iPad mais après avoir investi autant dans ce petit bout de plastique, on a forcément la hantise de l'oublier dans un coin et de voir un inconnu fureter dedans. Au revoir vos données, vos comptes mails, etc. Apple a heureusement pensé à proposer une option permettant de protéger l'intégralité des données avec un mot de passe. En cas de vol, ce type de protection peut même devenir une source de motivation supplémentaire pour vous le retourner... Allez tout d'abord dans **Réglages, Général** puis **Verrouillage par code**. Entre un nombre à 4 chiffres que vous pourrez aisément vous rappeler et éteignez la machine. Tel un code PIN, l'appareil vous demandera ce code à chaque démarrage. Il est aussi possible d'activer l'option **Effacer les données** qui effacera toutes les informations au bout de 10 codes erronés. Radical mais efficace.

Effacer complètement un disque dur avec CHAOS Shredder

La suppression d'un fichier ou d'un dossier laisse des traces sur votre disque dur et ces données peuvent être récupérées grâce à des logiciels spécialisés... même après avoir vidé la corbeille. De même un formatage laisse toujours des traces sur un disque dur. Le seul moyen d'effacer complètement un disque dur est de faire un formatage de bas niveau. CHAOS Shredder est le logiciel idéal pour cette tâche puisqu'il efface complètement les fichiers en réécrivant plusieurs fois des données quelconques à l'emplacement préalablement alloué aux fichiers concernés. Cette technique rend impossible toute récupération ultérieure par des méthodes logicielles ou matérielles.

 <http://safechaos.com>



TOP SERVICES PIRATES



NEWSGROUPS

USENEXT > Usenet tout confort !

Nous vous avons déjà parlé de Usenet, cet ensemble de protocole qui sert à la fois de forum de discussion et de forum d'échange de fichiers. Sachez que UseNeXT revient sur le devant de la scène en proposant une période d'essai de 14 jours complètement gratuite durant lesquels vous pourrez leecher 300 Go de données ! Pour en profiter il suffit de se munir de sa carte bancaire et de ne surtout pas oublier de résilier avant la fin de la période d'essai. Libre à vous de continuer l'aventure ensuite...

www.usenext.fr

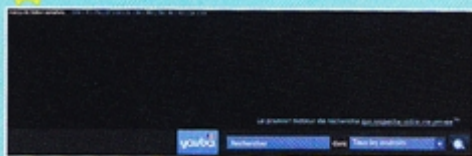
UseNeXT

MOTEUR DE RECHERCHE

YAUBA > Recherche anonyme

La particularité de ce moteur de recherche est de respecter votre vie privée : en effet rien n'est sauvegardé ni du côté du moteur de recherche (les fameux "logs") ni du côté client (pas de cookies !). Yauba permet aussi de visiter un site internet de manière anonyme suite à une recherche. Bien sûr, la navigation en est un peu ralentie, mais la confidentialité est une contrepartie qui vous laisse accepter ce petit désavantage. On peut aussi noter la grande qualité des recherches car, comme vous pourrez le constater, ce petit robot met son nez partout (sites Web, flux RSS, blogs, images, vidéos, documents Word, documents PDF, documents Power Point, réseaux sociaux, etc.)

<http://fr.yauba.com>

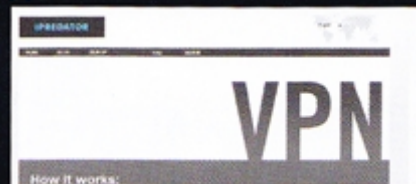


VPN

IPREDATOR Téléchargement anonyme

Lorsque la loi IPRED (Intellectual Property Rights Enforcement Directive) est entrée en vigueur en Suède, The Pirate Bay a immédiatement sorti son service IPREDator ! Il s'agit d'un VPN (Virtual Private Network) qui permet aux internautes de rester anonymes en utilisant un réseau privé virtuel. En effet la question de l'adresse IP est la clé de voûte des débats qui agitent en ce moment les pays européens (HADOPI, etc.) Le site de IPREDator est clair : « nous ne stockons aucune donnée de trafic ». Par contre la tranquillité a un prix : 15 € pour 3 mois...

www.ipredator.se



MULTIMÉDIA

TOP

MIDOMI Recherche de chansons

Vous avez une chanson qui vous trotte dans la tête, mais malheureusement vous ne connaissez pas son auteur ou son titre... Pour retrouver ces informations, il suffit d'essayer Midomi ! Chantez ou sifflez votre air dans un micro et la communauté vous aidera à retrouver cette chanson et à en trouver d'autres du même acabit...

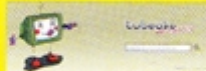
www.midomi.com



TUBEOKÉ Karaoké

Il fallait y penser, YouTube est certainement le plus grand réservoir de clips musicaux au monde. Les inventeurs de TubeOke en ont donc profité pour utiliser ces vidéos sous forme de Karaoké. Faites votre recherche parmi les vidéos de YouTube et les paroles apparaissent sur le côté. De quoi animer les soirées !

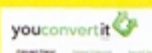
www.tubeoke.com



YOUCONVERTIT Conversion de fichiers

YouConvertit permet de convertir facilement, rapidement et gratuitement des fichiers documents, images, audio ou vidéo en ligne sans télécharger la moindre application. Il suffit d'uploader votre fichier, déterminer le format de conversion et saisir votre adresse email pour recevoir le fichier converti. YouConvertit permet également de faire des conversions de mesure !

www.youconvertit.com



TESTS EN LIGNE

PC FLANK Testez votre firewall

Ce site en anglais permet de tester la configuration de votre firewall sans installer quoique ce soit. Le site scan les ports un à un et vérifie que tout est en ordre. Il existe aussi d'autres services sur cette même page qui seront susceptibles de vous aider : test de connexion, antivirus, test de votre navigateur et de votre anonymat, etc.

www.pcfank.com



POUR TOUS VOS BESOINS,
TOUTES VOS ENVIES

HORS SÉRIE N°3 **100% PRATIQUE** 2[€],90

webpocket

HORS SÉRIE

AOÛT-SEPTEMBRE 2010

TÉLÉCHARGER FILMS, SÉRIES, MUSIQUE & JEUX

» LES MEILLEURS
LOGICIELS, SITES
ET SERVICES

GRATUITS !

**GUIDES PAS À PAS
+ TRUCS & ASTUCES**

- > BITTORRENT
- > MEGAUPLOAD
- > TÉLÉCHARGER
LE STREAM
- > RÉSEAUX
ANONYMES
- > PEER-TO-PEER
- > LES MEILLEURES
OFFRES VOD
- > USENET
- > ET LES JEUX
ALORS ?

HADOPI :
LES RÉSEAUX
CONTRÔLÉS ET CEUX
QUI ÉCHAPPENT
À LA SURVEILLANCE



2[€],90



LE MEILLEUR DU WEB !

**LES PIRATES CRYPTENT,
NOS LECTEURS
DÉCRYPTENT !**

PIRATE
INFORMATIQUE

**LE HACKING
EN PRATIQUE :**

**LES DERNIERS LOGICIELS, CRACKS,
ASTUCES, ALERTES ET TENDANCES
POUR SAVOIR, SE PROTÉGER ET AGIR**