SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

Site : http://aviquesnel.free.fr/Mederic
www.club-mederic-marseille.org (site du club)

23 mars 2009
Numéro 96

Sommaire

Bouclier anti-malware Threatfire

L'objectif de **ThreatFire** est de protéger votre PC de toutes attaques potentielles, virus, vers, trojans, rootkits et autres. Il intègre des outils vous permettant de vous défendre sans connaissances particulières en informatique.

En effet **ThreatFire** agit comme un antivirus, équipé d'une protection résidente qui analyse, détecte et bloque en temps réel, les processus dont l'activité est nocive pour la stabilité de votre système.

Ce qui distingue **ThreatFire** d'un antivirus est sa méthode de détection basée sur un système intelligent n'utilisant pas de signatures virales. Cet atout lui permettrait en théorie d'être plus efficace que n'importe quel autre antivirus sur le marché. En effet, son filtre de protection n'est pas un simple système de détection par comparaison, mais une détection basée sur la recherche d'activités potentiellement dangereuses. Il pourrait ainsi vous prémunir de virus encore inconnus et de plus, selon l'éditeur, des spywares.

En plus de la protection en temps réel, la version gratuite vous donne la possibilité d'effectuer un scan complet de votre ordinateur afin **d'éliminer**

les rootkits et seulement les rootkits.

Un rootkit est un programme ou ensemble de programmes permettant à un tiers (un pirate informatique, par exemple, mais pas nécessairement) de maintenir - dans le temps - un accès frauduleux à un système informatique.
Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée afin de camoufler tous les changements effectués lors de l'intrusion. C'est comme cela que l'on peut préserver l'accès à la machine un maximum de temps. Les rootkits sont ainsi difficilement détectables et seule une analyse approfondie peut en révéler la présence.

L'inconvénient majeur de cette version gratuite, est qu'elle ne propose pas de scanner pour les virus.
Pour cela vous devez utiliser votre antivirus habituel Avast ou AVG.

Vous pourrez tout de même l'utiliser en complément de vos antivirus, pare-feu et antispyware, puisqu'il peut parfaitement cohabiter avec tout autre programme de sécurité sans entrer en conflit. **ThreatFire** est donc un complément idéal permettant d'assurer une meilleure sécurité de votre PC.

L'avantage de cette application est qu'elle est très discrète et sans impact sur les performances de votre ordinateur, puisqu'elle n'utilise que 28 Mo de mémoire vive.

ThreatFire génère un rapport et des statistiques de protection, et dispose également d'un système de mise à jour automatique.

Comment ThreatFire peut-il me protéger lorsqu'un antivirus ne le peut pas ?

ThreatFire protège en permanence votre ordinateur contre les attaques en détectant les comportements malveillants, tels que l'enregistrement des données saisies au clavier ou le vol de données plutôt qu'en recherchant des menaces connues, comme le font les antivirus traditionnels. Étant donné qu'il intègre un système d'analyse comportementale en temps réel, **ThreatFire** est capable de bloquer de nouvelles menaces jamais rencontrées auparavant, simplement en détectant leur comportement malveillant.

Les nouvelles menaces qui apparaissent sont généralement conçues pour exploiter de nouvelles failles de sécurité ou vulnérabilités connues non encore couvertes par les solutions de sécurité traditionnelles. Elles se répandent généralement rapidement grâce à l'envoi en masse d'emails (SPAM), par détournement de sites Web, par messagerie instantanée ou via les réseaux d'échanges de fichiers en P2P. Étant pratiquement indétectables, elles ont l'occasion de causer de nombreux dégâts et de compromettre la sécurité des ordinateurs qu'elles contaminent, et cela même sur des ordinateurs équipés d'un antivirus à jour.

La technologie Active Defense™ vous offre une protection contre tous types de menaces, connues et inconnues : logiciels espions, logiciels publicitaires, enregistreurs de frappe, virus, vers, chevaux de Troie, rootkits, dépassements de mémoire tampon et autres logiciels malveillants.

Cas détectés — Liste des menaces récentes les plus courantes contre lesquelles

ThreatFire vous protège, liste des menaces actives et bien plus encore… Les menaces répertoriées sont celles détectées par ThreatFire au sein de sa communauté d'utilisateurs. Sélectionnez une menace pour afficher sa répartition géographique actuelle au sein de la communauté ThreatFire. Cliquez sur le lien « En savoir plus sur cette menace » pour afficher les rapports détaillés sur la menace produits par notre système d'analyse automatisé, ThreatExpert.

Logiciels malveillants	Logiciels publicitaires
Trojan-Downloader.Small!sd6	
Win32.Sality.AM.Gen	
Trojan.Lineage.Gen!Pac.3	
Email-Worm.Brontok!sd5	
Worm.AutoRun!sd6	
Win32.Virut.Gen.4	
Trojan-Downloader.Small.CQB	
Worm.AutoIT.V	
Worm.Hamweg.Gen	
Application.Ardamax_Keylogger	

Logiciels malveillants	Logiciels publicitaires
Adware.HotBar	
Adware.GameVance	
Adware.WhenU_SaveNow	
Adware.Trymedia.E	
Adware.Agent	
Adware.Craagle!sd5	
Adware.Thingies!sd5	
HTML.Psyme.Gen	
Backdoor.IRCBot	

Pourquoi mon antivirus ne peut-il pas bloquer les attaques récentes ?

Les attaques récentes surviennent plus rapidement que ce à quoi les antivirus traditionnels sont capables de faire face. Voici ce qu'un antivirus traditionnel utilisant une détection basée sur les signatures doit faire pour vous protéger contre une nouvelle menace :

1. Capturer une menace.
2. Analyse d'une menace pour comprendre son fonctionnement.
3. Écrire une signature permettant de reconnaître la menace.
4. Tester la signature pour s'assurer qu'elle n'endommage pas l'ordinateur.
5. Reçoit une mise à jour avec la nouvelle signature. Puis…
6. Vous devez toujours mettre à jour votre logiciel avec la nouvelle signature !

Certains éditeurs de solutions antivirus peuvent parfois prendre plusieurs jours avant de fournir une mise à jour des bases de signatures antivirales nécessaires pour protéger votre ordinateur. De plus, l'utilisation de signatures traditionnelles ne peut pas vous protéger contre les menaces « mutantes » qui changent de forme pour échapper à l'identification par signature.

Si j'utilise ThreatFire, puis-je désinstaller mon antivirus actuel ?

Aucune application n'étant absolument parfaite, une défense basée sur plusieurs niveaux de protection est toujours préférable. ThreatFire est un complément de votre antivirus actuel, et il saura vous protéger entre les périodes de mise à jour de votre antivirus.

Il est compatible avec les antivirus traditionnels et peut fonctionner en même temps sans provoquer de conflit.

Le scanner de ThreatFire est-il comme ceux des antivirus traditionnels ?

Lorsque vous lancez le scanner de rootkits de ThreatFire, ne vous attendez pas à voir des résultats comparables à ceux d'un antivirus ou d'une solution anti logiciels espions traditionnels. La protection offerte par ThreatFire est essentiellement un protection en temps réelle, aucun scan n'est nécessaire. Il contrôle en permanence l'activité de votre PC pour détecter tout comportement malveillant. Contrairement aux antivirus traditionnels, aucun scan n'est nécessaire pour détecter les logiciels malveillants. ThreatFire vous alertera immédiatement dès qu'une menace est exécutée et il donnera de nombreuses indications sur le comportement malveillant détecté.

Vous remarquerez toutefois que ThreatFire inclut un scanner de rootkits. Ce scanner analysera l'ordinateur pour y rechercher les rootkits cachés les plus difficiles à détecter.

Le scanner de rootkits de ThreatFire est conçu pour compléter la protection principale par analyse comportementale de ThreatFire.

Qu'est-ce que le rapport des statistiques de protection ?

La section Statistiques de protection (également appelée rapport des statistiques de protection) présente les onglets Protection personnelle et Protection communautaire. Vous pouvez afficher ce rapport à tout moment en accédant au panneau de configuration puis en sélectionnant l'onglet Statistiques de protection. En outre, il est affiché toutes les deux semaines pour vous informer de l'état de votre protection. Si vous le souhaitez, vous pouvez désactiver cette création de rapport automatique dans la section Paramètres généraux.

L'onglet Protection personnelle donne des informations sur la façon dont ThreatFire protège votre ordinateur. L'onglet Protection communautaire donne des informations sur la façon dont ThreatFire protège l'ensemble des membres du réseau Secure Community.

Les éléments suivants sont inclus dans les rapports :

Événements analysés – Nombre d'évaluations d'actions réalisées par ThreatFire pour déterminer s'il s'agissait d'une action potentiellement dangereuse.

Programmes analysés – Nombre de processus surveillés ou analysés par ThreatFire pour déterminer s'ils présentent des comportement suspects.

Activités suspectes détectées – Nombre de fois pour lesquelles ThreatFire a signalé un processus potentiellement dangereux.

Logiciels malveillants bloqués – Nombre de fois pour lesquelles ThreatFire a détecté et bloqué un logiciel malveillant.

Que se passe-t-il lorsque ThreatFire détecte une menace ?

Lorsque ThreatFire détecte une attaque de l'ordinateur par une menace connue, il la termine immédiatement et isole le logiciel malveillant concerné. Une alerte s'affichera alors pour confirmer que ThreatFire a bloqué l'attaque.

Il suffit de cliquer sur « Continuer » pour revenir au point auquel vous étiez avant l'attaque.

Que se passe-t-il lorsque ThreatFire détecte un « processus potentiellement dangereux » ?

S'il détecte une activité pouvant *probablement* être considérée comme une attaque, il suspend immédiatement le processus suspect et vous avertit que l'ordinateur est en danger.

Examinez les informations indiquées par ThreatFire afin d'autoriser le processus ou de le placer en quarantaine. Cliquez sur le lien « Détails techniques » pour afficher une liste des fichiers ou objets du registre placés en quarantaine par ThreatFire. Cliquez sur le lien « En savoir plus sur cette menace » pour obtenir plus d'informations et prendre une décision. Demandez à ThreatFire de mémoriser votre réponse en cochant la case « Mémoriser cette réponse ».

Sur quels critères dois-je décider d'autoriser ou de mettre en quarantaine ?

Vous devez tout d'abord examiner attentivement les informations fournies par l'alerte qui s'affiche : regardez en particulier les sections « Que se passe-t-il », « Degré de risque » et « Type de menace ». Ces informations vous aideront à déterminer ce qui se passe. Vous pouvez également cliquer sur le lien « En savoir plus sur cette menace » pour lancer une recherche Web sur le véritable nom de la menace. Cette recherche vous permet généralement de savoir de manière sûre si un processus est un logiciel malveillant ou un programme inoffensif.

Il est probablement acceptable de cliquer sur « Autoriser » pour une alerte s'il s'agit d'un programme que vous connaissez et auquel vous faites confiance et si vous venez juste de lui demander de réaliser une tâche spécifique. Par exemple, si vous désinstallez un programme ou que vous recevez une mise à jour d'un programme auquel vous faites confiance, il se peut qu'une alerte soit affichée dès que vous réalisez une de ces actions. Dans de tels cas, il n'est généralement pas très risqué de cliquer sur « Autoriser ».

Toutefois, si vous ne venez pas de réaliser une action ou s'il s'agit d'un programme auquel vous ne faites pas entièrement confiance, il est préférable de cliquer sur « Quarantaine ». Il est toujours possible de restaurer un élément placé en quarantaine depuis le Centre de contrôle des menaces si vous le souhaitez.

À quoi sert la case d'option « Mémoriser cette réponse » ?

Lorsque vous cochez la case « Mémoriser cette réponse », ThreatFire mémorise votre réponse pour ce processus afin d'autoriser cette action par la suite sans avoir à vous interroger de nouveau. À l'avenir, aucune alerte ne s'affichera pour ce même processus et pour cette même action (à condition de cocher la case).

Attention, vous ne devez cochez la case « Mémoriser cette réponse » pour autoriser un processus uniquement si vous êtes absolument certain qu'il est sûr. Toutefois, vous pouvez toujours changer d'avis en utilisant le Centre de contrôle des menaces de ThreatFire.

Et si je souhaite changer d'avis plus tard ?

Dans certains cas, lorsque vous décidez de toujours autoriser une action spécifique, il se peut que vous vous rendiez compte ultérieurement qu'il serait préférable de l'interdire (ou inversement). Le cas échéant, accédez simplement au Centre de contrôle des menaces depuis le panneau de configuration de ThreatFire. Depuis cette section, vous pouvez facilement annuler toute action précédente en supprimant l'entrée correspondante dans la liste Autorisés ou Refusés, ou en restaurant une entrée depuis la liste Quarantaine.

Que se passe-t-il lorsque ThreatFire détecte un logiciel publicitaire ?

Certaines applications ne sont ni clairement dangereuses ni clairement inoffensives, mais se situent quelque part entre les deux dans une sorte de « zone grise ». ThreatFire appelle ces logiciels des « applications potentiellement indésirables » ou API. Les API peuvent être aussi bien des logiciels publicitaires que des outils d'administration, voire d'autres types d'outils.

Bien que les logiciels publicitaires soient conçus pour afficher des publicités à un format spécifique, ils sont parfois livrés avec d'autres programmes que vous souhaitez réellement installer. Le choix d'exécuter ou non ces logiciels publicitaires vous appartient alors.

FSecure Exploit Shield pour Internet Explorer

Comme Symantec et ses "Norton Labs", les F-Secure Labs ont choisi (depuis très longtemps) de faire découvrir à tous les nouvelles défenses sur lesquelles ils travaillent avant de les intégrer dans leurs prochaines suites. La dernière production des F-Secure Labs s'appelle "F-Secure Exploit Shield". Ce nouveau bouclier bloque les "malwares" avant qu'ils ne s'installent en parant leurs attaques sans utiliser de signature. "F-Secure Exploit Shield" s'est ainsi révélé très efficace pour bloquer le premier code exploitant la toute dernière faille d'IE7 dont le patch a été rendu public il y a quelques jours.

F-Secure Exploit Shield est un bouclier qui agit en temps réel lorsque vous naviguez sur le Web, et vous protège contre toutes les techniques d'infiltration basées sur une compromission du navigateur.

Le logiciel est pour l'instant gratuit (c'est une version Bêta, réservée à un public confirmé et averti), en anglais, compatible XP et Vista (uniquement en 32 bits).

- Commencez par télécharger "F-Secure Exploit Shield" depuis le site de l'éditeur: <ici>

- Une fois installé, le logiciel manifeste sa présence par l'apparition d'une icône F-Secure en zone de notification (près de l'horloge) .

- Double-cliquez sur cette icône pour afficher l'interface du logiciel.

- "F-Secure Exploit Shield" comporte en réalité deux boucliers temps réel:
** Vulnerability Shields protège le système contre les attaques portant sur les vulnérabilités connues et non patchées par l'utilisateur (votre ordinateur est protégé même si vous n'avez pas fait de petit tour sur "Windows Update" depuis un moment).*
** Proactive Measures bloque tout comportement malveillant de la page visitée et des codes qu'elle héberge (il vous protège donc si la menace n'est pas connue par votre antivirus).*

- La proteciton est totalement automatisée. Dès qu'une attaque est détectée, l'accès au site Web et bloqué et une page d'alerte est affichée.

Remarque:
"F-Secure Exploit Shield" ne vous dispense pas d'un bon antivirus, d'un pare-feu ou d'une suite de sécurité. C'est juste une protection supplémentaire, particulièrement essentielle si votre ordinateur est protégé avec une suite un peu ancienne ou par des outils gratuits.

Organiser votre bureau avec Fences

Fences vous aide à "nettoyer" votre bureau en organisant les icônes. En effet, le logiciel rassemble automatiquement ces dernières à l'intérieur de groupes (dossiers, logiciels, favoris, etc.) séparés par des cadres. Chacun de ces cadres peut ensuite être personnalisé (changement de position, modification de taille, etc.). Par la suite, un simple double-clic sur le bureau suffira pour afficher les icônes ou les masquer !

Fences vous aide à *"nettoyer"* votre bureau en rassemblant automatiquement vos icônes au sein de groupes bien distincts et automatiquement agencés.
Téléchargez et installezl'application **Stardock Fences** depuis ce lien.

Au premier lancement le logiciel vous propose soit de choisir une mise en page prédéfinie pour vos icônes (**Start using Fences**), soit d'accéder directement au module de création d'une mise en page (**I'll create my fences on my own**).

- Cliquez sur **Start using Fences**
- Le logiciel vous demande ensuite si vous souhaitez démarrer avec une mise en page simplifiée composée uniquement de deux groupes (**Just create a couple fences**), ou si vous préférez que le logiciel ordonne automatiquement vos icônes selon différents groupes (**Sort out my icons**). Si votre bureau est très encombré, cliquez sur **Sort out my icons**.

- Puis cliquez sur **Open Fences Settings**. La boîte de paramétrages s'ouvre. Elle comporte 6 onglets:

* **Onglet Fences**: cet écran vous permet de pré-positionner les groupes à l'écran pour un alignement esthétique. Il suffit de choisir l'un des 7 agencements proposés par le menu *"Choose Layout"*.

* **Onglet Customize**: là, vous pourrez indiquer la teinte du groupe ainsi que son degré de transparence.

* **Onglet Tools**: cet onglet donne accès au mode *"Snapshot"*. Cette fonction permet de mémoriser un agencement d'icônes et de groupes, et de le rappeler à volonté. Signalons que Fences réalise un *"snapshot"* de votre bureau avant son installation ce qui permet de retrouver à tout moment son bureau d'origine simplement en cliquant sur **Pre-Install Snapshot**.

- Une fois tout convenablement paramétré, sachez qu'**il suffit de glisser/déposer une icône dans un groupe pour l'y ranger**. Les icônes au sein d'un groupe se réordonnent toutes seules. Les groupes peuvent être déplacés et positionnés où bon vous semble, à l'aide de la souris, en cliquant sur leur barre de titre.

- **Vous pouvez faire disparaître d'un seul coup tous les groupes** (et icônes) tout simplement **en double-cliquant sur le bureau**. Il est même possible de spécifier que certains groupes ne doivent jamais être cachés par cette méthode: il suffit de cliquer du bouton droit sur un groupe et de sélectionner "**Exclude this Fence from quick-hide**".

- Pour changer le nom d'un groupe, cliquez dessus du bouton droit de la souris et sélectionnez **Rename Fence**.

- Pour créer un groupe supplémentaire, cliquez du bouton droit sur le bureau, sélectionnez **Edit Fences**, vérifiez que l'onglet **Fences** est bien sélectionné et cliquez sur le lien **Create a fence**.

Street View : plus de 30 villes françaises désormais exposées

Après avoir été lancé en octobre 2008 pour Paris, Lyon, Marseille, Toulouse, Lille et Nice, le service Street View s'étend aujourd'hui à 26 nouvelles agglomérations. Ce qui porte désormais à 32 le nombre de villes françaises disponibles dans le service de visualisation des rues à 360 degrès de Google. Parmi les nouveaux venus figurent Nantes, Rennes, Strasbourg, Montpellier ou encore Saint Malo.
Disponible sur le service de cartographie Google Maps, Street View permet de naviguer virtuellement au niveau des rues photographiées par Google. L'internaute peut ainsi localiser un commerce, un hôtel, le quartier de son futur appartement, ou, comme le suggère Google, "apprendre à mieux connaître le patrimoine français".

Rennes sur Google Street View - Cliquez ici pour agrandir l'image

Lancé en mai 2007 pour San Francisco, Street View est aujourd'hui disponible dans plus de 50 villes américaines, ainsi que plusieurs villes d'Europe, d'Australie et du Japon. En France, il concerne désormais plus d'une trentaine de villes.

Les utilisateurs de Street View peuvent dès à présent explorer les villes de Nantes, Strasbourg, Montpellier, Rennes, Le Havre, Reims, Saint Etienne, Toulon,

Cannes, Grenoble, Angers, Dijon, Brest, Amiens, Aix en Provence, Limoges, Dunkerque, Saint Malo, Troyes, Châlons-en-Champagne, Calais, Rouen, Caen, Poitiers, Clermont-Ferrand et Valence.

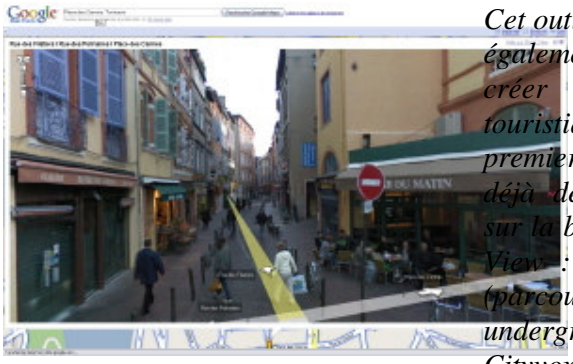
De plus, Google précise que la couverture des six premières villes françaises (Paris, Lyon, Marseille, Toulouse, Lille et Nice) a été étendue à leurs périphéries.

Pour profiter de Street View, il suffit de déplacer le petit bonhomme orange qui se trouve en dessous de la commande de navigation sur Google Maps, et de le poser sur les rues qui apparaissent en bleu.

Site : http://maps.google.fr

Complément d'actualité

Les villes françaises désormais visibles sur Google Street View : Google a officialisé mercredi 15 octobre le lancement en France de Street View, un service qui permet de visualiser une ville à 360 degrés depuis la route. Jusque-là disponible aux Etats-Unis, au Japon et en Australie, cette fonctionnalité à Google Maps débarque pour la première fois en Europe. Les internautes peuvent dès à présent visualiser Paris, Lille, Marseille, Nice, Lyon et Toulouse en photos haute résolution.



La Place des Carmes à Toulouse - Cliquez sur l'image pour agrandir

Google Street View se présente sous la forme d'une fonctionnalité intégrée à l'interface Google Maps. Sur la carte, des petits icônes représentés par un petit appareil photo indiquent les zones couvertes. En cliquant sur ces modules, l'internaute peut visualiser le terrain en images dans une fenêtre. Il peut alors naviguer sur la rue ou la route photographiée, reculer, tourner pour visualiser la façade d'un immeuble ou admirer un monument.

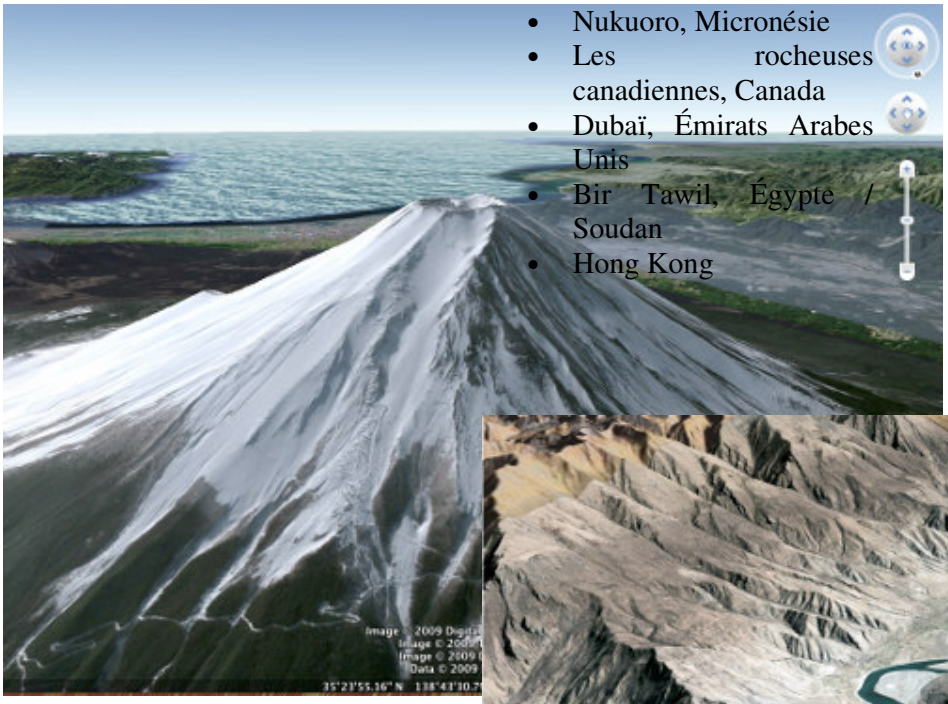
Face aux critiques sur le respect de la vie privée aux Etats-Unis mais aussi en France, Google a également conçu un logiciel capable de flouter le visage des personnes photographiées ainsi que des plaques d'immatriculation. "Cette nouvelle technologie de floutage est très performante, mais il se peut que quelques visages n'aient pas été floutées. Si c'est le cas, les internautes peuvent demander de retirer une photo et Google agira dans les délais les plus rapides" assure Luc Vincent, en déplacement à Paris pour l'inauguration en Europe de Street View.

Cet outil cartographique permet également aux entreprises de créer des applications touristiques ou culturelles. Cinq premiers partenaires proposent déjà des services géolocalisés sur la base des photos de Street View : le magazine Télérama (parcours du Paris underground et insolite), Cityvox (restaurants préférés des internautes), TVtrip (visites des hôtels), Drimki (visualisation des biens immobiliers) et l'Office du Tourisme et des Congrès de Paris (découverte des monuments de la capitale).

Les premières images du satellite GeoEye-1 de Google dans Google Earth

De bien belles images en haute résolution...

Le 6 septembre dernier, GeoEye-1 a été placé en orbite à 660 kilomètres au dessus de nos têtes. Ce satellite commercial, capable de prendre en photo des détails de 41 centimètres, était financé en partie par Google. La firme californienne, qui avait fait même fait apposer son logo sur la fusée, avait en effet acquis les droits d'utilisation des photographies prises avec ce satellite.



Mont Fuji, Japon.

Aujourd'hui, Henri Willox nous apprend que Google a mis en ligne pour la première fois des images prises par GeoEye-1. Pour les consulter, il vous suffit de télécharger ce fichier KML et de l'ouvrir avec le logiciel Google Earth.

Voici la liste des vues de GeoEye-1 disponibles dans Google Earth :

- Arcachon, France
- Mont Fuji, Japon
- Tokyo, Japon
- Alexandrie, Égypte
- Le Caire, Égypte
- Barcelone, Espagne
- Malpica, Espagne
- Le Cap, Afrique du Sud
- Bornéo, Indonésie
- Cabo Polonio, Uruguay
- Cayos Miskitos, Nicaragua
- Sydney, Australie
- Région autonome du Tibet, Chine
- Fuzhou, Chine
- Nukuoro, Micronésie
- Les rocheuses canadiennes, Canada
- Dubaï, Émirats Arabes Unis
- Bir Tawil, Égypte / Soudan
- Hong Kong

Le Xizang (Tibet) vu par le satellite GeoEye-1 et mis en relief par Google Earth

Internet Explorer 8 officiel et disponible

IE 8 est arrivé, la toute dernière version du navigateur Web de Microsoft est disponible au téléchargement sur le site du géant de l'informatique. Depuis quelques semaines déjà, les rumeurs se faisaient plus précises sur l'avancée des travaux de la version finale.

Téléchargez Internet Explorer 8

La décision a sans doute été forcée par les récents chiffres, plutôt mauvais pour Internet Explorer, et qui montraient la baisse croissante des parts de marché du navigateur leader du marché. En attendant le passage en revue des nouveautés de cette nouvelle version, voici les liens pour tester Internet Explorer 8. Petit rappel : IE8 est incompatible avec la version bêta de Windows Seven.

Télécharger Internet Explorer 8 pour Windows XP

Télécharger Internet Explorer 8 pour Windows XP (64)

Télécharger Internet Explorer 8 pour Windows Vista

[Télécharger Internet Explorer 8 pour Windows Vista (64)]

Vista ne gère que 3 Go ? La légende expliquée

Vous avez sûrement déjà entendu la phrase « Vista ne gère que 3 Go de RAM ». Cette légende urbaine (car c'est totalement faux) a la dent dure et nos collègues de Tom's Hardware ont donc décidé d'expliquer le pourquoi du comment. Vous voulez savoir pourquoi votre Windows ne reconnaît que 3,5 Go de RAM sur 4 Go ? Pourquoi Mac OS X, un système 32 bits, permet de travailler avec 8 Go de RAM 4 Go, 3,5 Go, 3,12 Go ?

Un des problèmes les plus courants vient de la limitation de la RAM : même avec 4 Go de RAM, on se retrouve avec 3 Go (et des poussières utilisables). Explications. Les périphériques (cartes sons, contrôleurs de stockage, cartes vidéo, etc.) nécessitent une zone mémoire pour être accessibles. En x86, cette zone mémoire est placée dans la mémoire adressable, donc dans les 4 Go adressables. Bien évidemment, un programme ne doit pas pouvoir aller écrire dans ces zones, qui sont réservées. Avec Windows 2000 et Windows XP sans SP (ou SP1), il est possible de déplacer ces zones hors des 4 Go, en utilisant le PAE (qui est optionnel avec ces OS) et donc de disposer de 4 Go de RAM utilisables quand on dispose de 4 Go de RAM physiques. Avec Windows XP SP2 (et SP3), Microsoft a activé le PAE sur toutes les machines et les premiers tests ont montré que certains pilotes n'appréciaient pas ce mode d'adressage et provoquaient des écrans bleus. Il a donc été décidé de bloquer son usage et de placer l'adressage des périphériques dans la zone utilisable : avec ces OS, la mémoire utilisable est donc tronquée par les zones réservées par les périphériques. En pratique, on perd entre 128 et 512 Mo à cause de la carte graphique (seule une partie de la mémoire vidéo nécessite d'être adressée), plus une quantité de mémoire qui varie selon la carte mère et les périphériques installés. Sous Windows XP SP2 (ou SP3), on a donc en général entre 3 et 3,5 Go utilisables sur 4 Go physiques. Sous Windows Vista (32 bits) sans SP, la mémoire utilisable est généralement limitée à 3,12 Go (parfois moins) pour les mêmes raisons que sous XP SP2. avec le SP1, Microsoft limite la mémoire de la même façon, mais l'OS affiche bien qu'il dispose de 4 Go de RAM, un moyen simple de faire passer la pilule.

EN RESUME :

Windows 2000, Windows XP, Windows XP SP1 : 4 Go physiques, 4 Go utilisables (avec PAE).

Windows XP SP2, Windows XP SP3 : 4 Go physiques, entre 3 et 3,5 Go utilisables (avec PAE).
Windows Vista : 4 Go physiques, maximum 3,12 Go utilisables (avec PAE).

Windows Vista SP1 :4 Go physiques, maximum 3,12 Go utilisables (avec PAE), 4 Go affichés.

.