Chapitre 1

Pourquoi choisir Firefox ?

« *Utilisez un autre navigateur.* »

C'est le conseil radical donné par l'US-CERT[1] aux utilisateurs d'Internet Explorer (IE). Il précise en outre qu'« IE est si intimement lié à Windows que les vulnérabilités dans IE fournissent aux pirates un accès significatif au système d'exploitation »[2]. Cet organisme prudent, neutre et modéré n'a pas pour habitude de crier au loup : s'il s'engage de manière aussi indiscutable (il a donné ce conseil huit fois en 2004), c'est parce qu'il y a péril en la demeure – et parce qu'un navigateur technologiquement supérieur existe désormais pour remplacer Internet Explorer.

Au cours de ce chapitre, nous allons d'abord vous montrer ce qui conduit le CERT, comme tant d'autres organismes liés à la sécurité[3], à se montrer aussi péremptoire et pessimiste à l'égard d'un logiciel emblématique de Microsoft, utilisé quotidiennement par des centaines de millions de personnes à travers le monde. Nous vous présenterons ensuite le meilleur des navigateurs internet : Firefox.

[1] *United States Computer Emergency Readiness Team* (« Équipe de réaction rapide aux urgences informatiques des États-Unis »), branche du *Department of Homeland Security* (« Ministère de la sécurité de la patrie ») américain. Tous ses communiqués sont disponibles sur `www.us-cert.gov` .

[2] `www.kb.cert.org/vuls/id/713878` . Nous expliquerons page 14 ce que signifie en pratique cette explication technique.

[3] Par exemple, le *SANS Internet Security Center* affirme que « continuer à utiliser Internet Explorer est comme jouer à la roulette russe ».

1.1 IE : un logiciel obsolète

Internet Explorer était prometteur lors de sa sortie en 1995 : il était gratuit, affichait rapidement les pages web et présentait plusieurs nouveautés par rapport au logiciel dominant (et payant) de l'époque, Netscape. Il ne tarda pas à s'imposer et, fin 2004, il était encore utilisé par 90 % des internautes.

« Que le meilleur gagne » et le meilleur a gagné ? Pas si vite... Ce qui a imposé IE, c'est avant tout le fait qu'il soit préinstallé d'office, gratuitement[4], sur chaque nouvel ordinateur équipé de Windows. Cette pratique a coûté à Microsoft plusieurs procès en concurrence déloyale – procès qu'il a perdus[5]. Ce qui a porté puis maintenu IE au firmament des navigateurs, c'est moins sa qualité que l'impossibilité de le concurrencer[6].

Car la qualité n'est pas le point fort d'Internet Explorer : le roi est nu.

a. Les symptômes

Hélas, ce qui agace quand on utilise IE n'est qu'un détail au regard des vrais enjeux. Les fenêtres de pub intempestives, le navigateur qui ouvre des sites que l'on n'a pas demandés, la fenêtre qui change de taille toute seule, le mode plein écran qui s'active comme par magie, les navigateurs qui s'ouvrent en rafale plus vite qu'on ne peut les fermer, la page de démarrage qui change toute seule, l'ordinateur qui ralentit au fil des mois sans qu'on sache pourquoi : tous les utilisateurs d'IE ont déjà rencontré ces désagréments. Mais ce n'est pas grand-chose – sinon un indice de la piètre qualité du logiciel, dont on attendrait au moins qu'il nous laisse maître de la machine.

[4]Plus exactement, son coût est inclus (ou caché, selon le point de vue) dans celui de Windows.

[5]Et qui lui ont coûté plus de 3 milliards de dollars.

[6]Aucune entreprise ne peut sérieusement espérer vendre un navigateur alors qu'IE est déjà présent et gratuit sur tous les PC. Nous verrons page 19 pourquoi Firefox échappe à ce raisonnement.

Ce qui affole les experts, et qui devrait intéresser les utilisateurs responsables, c'est qu'Internet Explorer est une *passoire* du point de vue de la sécurité. 250 attaques informatiques ont été trouvées pour exploiter ses faiblesses. 150 d'entre elles concernent spécifiquement la version 6, qui est la plus récente[7]. Mettre à jour votre ordinateur par Windows Update ne suffira pas à vous protéger : comme Microsoft met entre quelques semaines et quelques mois pour proposer des correctifs, plusieurs dizaines d'attaques sont disponibles à chaque instant pour compromettre votre PC. Installer le pack SP2 ne suffira pas non plus : il suffit de visiter une page web avec Internet Explorer pour courir le risque d'être automatiquement infecté par un virus (par exemple le cheval de Troie nommé *Phel*), même si votre ordinateur utilise Windows XP SP2.

Ne croyez pas que vous trouverez la sécurité dans l'anonymat de la masse, qu'on vous laissera tranquille parce que ce qui est précieux à vos yeux est probablement sans valeur pour un pirate. Le temps des attaques manuelles est révolu depuis longtemps : aujourd'hui ce sont des programmes qui se chargent de vous pirater, 24 heures par jour, tous les jours de l'année. Un seul pirate peut prendre le contrôle de millions d'ordinateurs sans se lever de son lit. Il n'aura même pas vraiment besoin d'être un crack : des outils de piratage clefs en main sont disponibles sur Internet.

Les « pirates » veulent trois choses : vous observer, vous escroquer, ou utiliser votre ordinateur à des fins illégales. Toutes ces activités ont un point commun : elles doivent rester cachées. Si votre ordinateur a été piraté, il y a fort à parier qu'on ne vous a pas mis au courant. Utiliser un antivirus, un pare-feu, un éradicateur de SPYWARES et un nettoyeur de la base de registres ne suffira pas toujours. Il est déjà trop tard.

Mais dans le fond, se faire pirater, est-ce vraiment grave ?

[7] Information du journal *Le Monde*, édition du 12 octobre 2004.

b. Les risques que vous courez

La majorité des sites web ne présentent aucun risque pour votre sécurité ; les sites mal intentionnés ne sont qu'une petite minorité. Malheureusement, vous ne disposez d'aucun moyen pour distinguer le bon grain de l'ivraie. Lorsque vous consultez avec IE un site malveillant, qui se présentera invariablement sous la forme d'un site « comme les autres », les risques que vous courez s'échelonnent du simple désagrément à la prison, en passant par la honte et la ruine.

La plupart des sites « pirates » se contentent d'installer sur votre ordinateur, via Internet Explorer, un *spyware* (autrement dit un MOUCHARD) qui fera un rapport régulier sur votre utilisation d'Internet. Sans vous prévenir, cela va de soi. Ces rapports, couplés à votre adresse électronique, se monnayent cher auprès des entreprises car ils permettent à ces dernières de pratiquer un marketing finement ciblé[8] – terme poli qui signifie qu'elles exploiteront l'espionnage de votre vie privée pour vous envoyer du SPAM[9]. Cette pratique est choquante et désagréable, mais pas dramatique. Vous n'avez rien à cacher, n'est-ce pas ?

Plus inquiétants sont les *keyloggers*[10], qui enregistrent toutes les touches sur lesquelles vous appuyez. On pourra ainsi lire le contenu des courriers électroniques que vous écrivez, les adresses de vos destinataires, le prénom de votre patron – ou de votre amant – mais aussi tous vos mots de passe et le numéro de votre carte bleue. Une FAILLE d'IE permet une variante tout aussi astucieuse : vous diriger vers un site en vous faisant croire que son adresse est celle d'un autre. De la sorte, vous pensez consulter un site respectable (votre banque, une grande enseigne de la vente par correspondance, etc.) alors qu'on ne cherche qu'à récupérer vos coordonnées bancaires.

[8] Les entreprises en question sont potentiellement toutes les entreprises qui utilisent la publicité pour se faire connaître.

[9] Que l'on appelle aussi « courrier électronique non sollicité » ou, de façon plus colorée, « pourriel ».

[10] Littéralement, « enregistreurs (*loggers*) de touches (*key*) ».

Les *spywares* utilisés pour le « marketing direct » et les *keyloggers* qui préparent des arnaques ne sont que le menu fretin. Le risque maximal est encouru avec les « chevaux de Troie », qui permettent de prendre le contrôle complet de votre ordinateur. Sauf exception, le but n'est pas de fouiller parmi vos photos de vacances, d'envoyer en votre nom un courrier d'insultes à toute votre famille ni de transférer vos économies vers un compte discret dans un paradis fiscal.

L'enjeu est plutôt de transformer votre PC en « zombie » afin de réaliser des opérations illégales. Cette pratique permet au pirate de rester anonyme (c'est votre PC qui héberge ses activités, pas le sien) et de faire travailler ensemble un nombre considérable d'ordinateurs partout dans le monde. La seule limite est alors l'imagination des vrais criminels : on a ainsi vu des pirates faire du chantage à de grands sites commerciaux. En effet, si des millions d'ordinateurs se connectent simultanément à un site, ce dernier, noyé sous ce trafic soudain, devient inaccessible[11]. Dès février 2000, les sites d'Amazon, eBay, CNN et Yahoo ont ainsi été paralysés pendant quatre heures. Microsoft, le FBI[12] et le CERT ont également été victimes de cette pratique. D'après une étude de l'université de Californie[13], 4 000 attaques de ce type ont lieu chaque semaine. Ce que recherche le pirate, c'est l'argent qu'il peut tirer du chantage. Le moyen de son chantage, c'est votre ordinateur.

Enfin, des pratiques moins élaborées peuvent vous causer directement de gros soucis : que pourriez-vous répondre à la justice si l'on trouvait sur votre ordinateur des films piratés, des chansons interdites ou des images pornographiques illégales, tous installés là à votre insu par un pirate ? Comment expliqueriez-vous que 10 000 spams soient envoyés, chaque jour, depuis votre ordinateur ? Et si votre ordinateur héber-

[11] Cette technique est appelée DDoS pour *Distributed Denial of Service*, « déni de service distribué ».

[12] Le célèbre *Federal Bureau of Investigation* des films américains.

[13] `www.cs3-inc.com/pk_whatisddos.html` .

geait un site web se faisant passer pour celui de la Banque de France ? Tout ceci peut être présent sur votre ordinateur sans que vous en ayez conscience. Il est très facile de dissimuler des documents sur une machine ; si un pirate est assez malin pour contourner toutes vos protections, il le sera encore assez pour ne pas éveiller votre attention.

c. Avis de forte tempête jusqu'en 2007

S'il est fréquent qu'un programme contienne des bugs, il est exceptionnel que ces derniers permettent aux pirates de compromettre totalement la sécurité de Windows indépendamment du pare-feu et de l'antivirus. Ce qui distingue Internet Explorer, ce n'est pas le nombre de ses bugs. C'est le rapport intime qu'il entretient avec les entrailles de Windows, qui transforme ce qui aurait pu être des bugs mineurs en vulnérabilités critiques. Ce défaut de conception[14] condamne IE à demeurer toujours une voie royale pour les attaquants.

Afin de se représenter le problème, il est commode d'utiliser l'image d'une ville fortifiée. La partie la plus précieuse de votre ordinateur, c'est-à-dire vos données (textes, photos, courriers électroniques, etc.), sera les maisons. Elles sont bâties sur un terrain, qui figure le système d'exploitation (Windows). La ville est entourée d'un mur (le pare-feu) qui tient les malandrins à l'écart. Pour vous permettre de communiquer avec le reste du monde (web, courrier électronique, messagerie instantanée, etc.), le mur s'arrête ici et là pour laisser la place à quelques routes (Internet Explorer, Outlook, Messenger, etc.). Ces dernières sont protégées par des gardes (votre antivirus) qui filtrent les entrées et les sorties. De temps à autre, ils fouillent aussi toutes les maisons (re-

[14] L'imbrication étroite de Windows et d'IE résulte d'un choix commercial et non technique : elle permettait à Microsoft de se défendre de pratiquer une concurrence déloyale à l'égard de Netscape en prétendant qu'IE est indissociable de Windows. Pour justifier cette affirmation, qui ne répond à aucune nécessité informatique, la technique a été mise au service de la propagande.

cherche de virus dans tous les fichiers). En apparence, vous pouvez dormir tranquille.

Ce que vous ne pouviez pas savoir, c'est que le terrain sur lequel vous avez bâti votre ville surplombe une ancienne carrière. De temps à autre, une portion de rue s'effondre (un énième bug est découvert dans Windows). Vous n'êtes pas prévenu de l'irruption de chaque nouveau trou dans votre ville, les gardes non plus, mais vous savez que la compagnie minière qui vous a vendu le lieu (Microsoft) vient régulièrement pour couler du béton dans les fosses et refaire gratuitement le revêtement de la rue (Windows Update). D'ailleurs, même si l'on vous prévenait, vous n'y pourriez pas grand-chose : vous ne pouvez pas réparer les fondations (Windows) vous-même, vous ne pouvez qu'attendre quelques semaines. Normalement, ce désagrément ne devrait toujours pas compromettre vos défenses extérieures. Mais si : chaque trou dans la ville communique directement avec une ouverture au-delà des remparts ! (La « route » IE étant « intimement liée » à Windows, si l'un s'effondre, l'autre aussi[15].)

Entre le moment où la rue s'effondre et celui où la compagnie minière vient réparer les dégâts, l'accès à votre ville est complètement ouvert à ceux des assaillants qui savent trouver leur chemin à travers les carrières (et à leurs amis ou clients). Toutes vos belles défenses sont impuissantes contre cette traîtrise. Vous ne pouvez pas gagner dans ces conditions.

Vous n'avez que deux options pour assainir votre situation. La première est de faire en sorte que les cavernes ne débouchent plus sur l'extérieur (vous passer d'Internet Explorer). La deuxième, bien plus pénible, est de reconstruire votre ville sur un terrain qui ne passe pas son temps à s'effondrer (autrement dit, changer de système d'exploitation[16]).

La compagnie minière veut bien vous vendre un autre ter-

[15] Une illustration frappante de ce problème est exposée sur la page `slashdot.org/article.pl?sid=01/12/11/2125224` (en anglais).

[16] La sécurité est bien meilleure avec Mac OS X ou Linux qu'avec Windows.

rain sur la concession *Longhorn* (promis-juré, cette fois-ci ce ne sera pas comme sur vos concessions 95, 98 et XP), mais il ne sera pas prêt avant 2007[17]. Vous êtes prié de patienter et de croiser les doigts...

Ou alors, vous pouvez prendre votre destin en main et passer dès aujourd'hui à Firefox !

1.2 Firefox : la cavalerie est arrivée

Firefox est le navigateur créé par la Fondation Mozilla, qui édite également un lecteur de courrier électronique[18] (*Thunderbird*), un composeur de pages web (*Nvu*) et un organiseur partagé (*Calendar*). La Fondation Mozilla édite également une suite logicielle, baptisée elle aussi Mozilla, qui regroupe tous ces programmes. Dans la suite de cet ouvrage, nous nous concentrerons uniquement sur Firefox.

La version 1.0 de Firefox est sortie le 9 novembre 2004, simultanément en 27 langues (dont le français), pour Windows (toutes les versions), Mac OS X et Linux. Un mois plus tard, le logiciel avait déjà été téléchargé par 10 millions de personnes, essentiellement des professionnels de l'informatique et des amateurs éclairés puisque les premières pages de publicité pour le logiciel ne sont parues dans la presse que le 2 décembre

[17] La prochaine version de Windows, baptisée *Longhorn*, tentera de fusionner complètement les technologies des systèmes d'exploitation grand public et professionnels de Microsoft, de façon plus approfondie qu'avec Windows XP. Ce système devait initialement voir le jour en 2003, puis en 2005 ; la date de 2007 est actuellement retenue :

`www.microsoft.com/windowsserver2003/evaluation/overview/roadmap.mspx`

Internet Explorer ne sera pas mis à jour d'ici là (information du journal *Seattle Times*, édition du 27 décembre 2004).

[18] Le programme de Microsoft permettant de lire le courrier électronique s'appelle Outlook.

en Allemagne[19] et le 16 décembre aux États-Unis[20].

Qu'est-ce qui a bien pu provoquer un tel engouement chez ces personnes, qui savent généralement ce qu'elles font ?

a. Sécurité, sérénité

La plupart des utilisateurs de Windows ne savent pas quelle menace Internet Explorer représente pour leur sécurité. En un sens, ils ont de la chance : ils ne se rongent pas les sangs à chaque fois qu'ils consultent le web. Pour ceux qui savent, changer de logiciel s'apparente à un retour à l'innocence. Firefox n'est pas, comme IE, victime d'une tare congénitale qui le ferait chuter à chaque fois que l'on découvre un bug dans Windows.

Néanmoins, aucun programme de cette ampleur ne peut prétendre être exempt de défauts. Ce qui compte à cette échelle, c'est la nature des bugs et la manière d'y réagir.

Il y a une excellente raison de penser que Firefox est structurellement moins bugué que la plupart des autres programmes : il n'a pas été écrit sous une intense pression commerciale, contrairement à bien des logiciels écrits dans les années 1990. À fonctionnalités identiques, développer un logiciel bien sécurisé exige beaucoup plus de temps que prendre des raccourcis en touchant du bois. En entreprise le profit passe souvent avant l'amour du travail bien fait, ce qui peut être considéré comme normal – tant que la contrepartie n'est pas votre sécurité. Libéré de toute contrainte budgétaire, le projet Firefox a été développé pendant pas moins de six ans avant de parvenir à la version 1.0 . Chacun de ses éléments a

[19] C'est la collecte de 48 000 € auprès de 2 403 contributeurs généreux qui a permis de publier une pleine page dans le *Frankfurter Allgemeine*. Vous pouvez la consulter en ligne à l'adresse

`mozilla.wattenscheid.net/firefox_faz_anzeige.pdf`

[20] Dix mille contributeurs ont versé au total $250 000 en dix jours, ce qui a permis de publier une double page dans le *New York Times*. Vous pouvez la consulter en ligne à l'adresse

`www.mozilla.org/images/nyt_ad_large_2004.png`

été rigoureusement pensé, écrit et testé. Ses fondations sont solides.

Lorsqu'un problème de sécurité est malgré tout découvert, l'équipe de Firefox le corrige systématiquement en moins de 24 heures. Cette rapidité exceptionnelle n'est pas seulement le signe que l'équipe est dévouée, compétente et tournée vers les utilisateurs ; cela signifie aussi qu'il est possible de réaliser pareil exploit. Et ceci, à son tour, n'est envisageable que parce que le programme est bien conçu. À long terme, l'amour du travail bien fait apporte quand même des avantages...

Cerise sur le gâteau : sur votre ordinateur, Firefox se répare tout seul. Il se connecte régulièrement au serveur central et vous propose de télécharger les mises à jour[21]. De la sorte, vous n'avez rien à faire pour utiliser en permanence un navigateur enfin sécurisé.

b. Des fonctionnalités innovantes

Firefox n'est pas qu'un navigateur sécurisé : il intègre de nombreuses innovations fort pratiques. Quelques-unes sont de celles qui donnent un coup de vieux aux logiciels qui en sont encore dépourvus. En voici un échantillon :

- Les ONGLETS (voir l'image page 65) vous permettent de consulter simultanément plusieurs sites web dans une même fenêtre[22]. C'est bien plus pratique que d'ouvrir autant de fenêtres que l'on trouve de pages intéressantes, ou de revenir plusieurs fois à une même page contenant des LIENS que l'on souhaite explorer.
- Une BARRE DE RECHERCHE (page 73) est intégrée au navigateur. Elle permet d'interroger directement votre MOTEUR DE RECHERCHE favori, mais aussi des dictionnaires, des sites d'enchères, des comparateurs de prix, etc.

[21] On peut désactiver cette fonction.

[22] De la même manière que l'on peut utiliser plusieurs feuilles de calcul dans une seule fenêtre d'un tableur (Excel par exemple).

– De très nombreuses extensions peuvent aussi être ajoutées à Firefox. Elles permettent par exemple de bloquer toutes les publicités (page 113), de revenir à la page précédente par un cliquer-glisser n'importe où sur la fenêtre (page 116) ou encore de prévisualiser les réponses de Google (page 114).

Vous pourrez ainsi personnaliser votre outil afin qu'il réponde complètement à vos attentes. Et vous pourrez également modifier son apparence (page 88) en choisissant les couleurs, le dessin des boutons et l'emplacement des menus. Désormais, vous êtes seul maître à bord.

c. L'anticyclone OSS s'installe sur l'informatique

C'est très intéressant tout cela, le navigateur sécurisé, les mises à jour automatiques, les onglets, les extensions, mais... combien ça coûte ?

Pas un sou. Et il n'y a pas de piège : le logiciel n'est pas financé par la publicité, on ne vous demandera pas votre adresse électronique pour vous spammer ensuite, il n'y a pas de questionnaire à remplir, pas de frais cachés : rien. Le programme est écrit par des informaticiens qui ont travaillé à ce projet sur leur temps libre, pour le plaisir ou par conviction.

Firefox n'est pas un cas isolé mais seulement l'un des premiers programmes mis à la disposition du grand public dans le cadre d'une initiative de type associatif qui s'appelle l'*Open Source Software*[23] (OSS). Elle regroupe des dizaines de milliers d'informaticiens dans le monde entier, qui travaillent de concert via Internet. Leur objectif n'est pas le profit, mais la création de logiciels de qualité.

Leurs motivations ne sont pas si difficiles à comprendre. Imaginez un boulanger passionné par son métier, qui aime pétrir sa pâte, faire lever lentement ses baguettes et sentir l'odeur du pain chaud. Il ne peut que se sentir révolté par la fadeur, la mollesse et l'uniformité des bouillies agglomérées

[23] Que l'on traduit par « logiciel libre » en français.

que les fourneaux industriels débitent à la chaîne. Ce qui le désole le plus, c'est que les gens oublient le goût du vrai pain ; qu'ils en viennent à confondre le produit de son art avec les clones anonymes qu'on leur sert à la cantine. De temps à autre, il réunit quelques confrères et amateurs éclairés pour parler du métier, goûter les dernières créations et échanger des recettes. À l'occasion, ils unissent leurs moyens et leurs efforts pour offrir tous ensemble une dégustation au public, afin de se faire plaisir, partager leur passion et montrer qu'il n'y a pas de fatalité, seulement de la volonté.

Comme notre boulanger, les informaticiens qui participent au mouvement OSS ont l'amour du travail bien fait. Mais loin d'être les gardiens d'un savoir-faire menacé, ils sont l'avant-garde d'une révolution high-tech qui change radicalement la manière de créer des logiciels. Leur terrain de jeu, c'est l'ordinateur, de l'orfèvrerie du processeur à l'alchimie des protocoles Internet. Leurs ingrédients sont gratuits : ce sont d'autres programmes qu'ils ont déjà écrits. Ils n'ont pas de stand à tenir : un site web s'en charge pour eux. Leurs créations ne sont pas périssables : au contraire, elles croissent et s'améliorent au fil du temps. Partout où la matière résiste et fait obstacle aux bonnes volontés, l'informatique est, à l'inverse, un allié qui amplifie les contributions de chacun.

Ce qui fait la force des bénévoles de l'OSS (qui sont généralement informaticiens de profession, ou de formation[24]), c'est qu'ils œuvrent ensemble. Parce que leurs programmes sont « ouverts »[25], chacun peut réutiliser tout ou partie du travail d'un autre. Un programme « fermé » ressemble à une pierre magique : il suffit de la toucher pour qu'elle accomplisse sa fonction, mais on ne saura jamais comment elle fonc-

[24] À la Fondation Mozilla, l'équipe des bénévoles est complétée par 40 programmeurs « prêtés » à plein temps par de grandes entreprises (IBM, AOL, Sun, etc.). Ces dernières font également des donations à la Fondation (plus de deux millions de dollars jusqu'à présent).

[25] C'est de là que vient l'expression *open source* : la « recette » d'un programme s'appelle son « code source » et c'est lui qui est ouvert (*open*) au public.

tionne. On ne pourra donc ni la réparer, ni l'améliorer. Un programme « ouvert » ressemble, lui, à un livre magique : il suffit aussi de le toucher pour qu'il fonctionne (en produisant les mêmes effets qu'un programme fermé), mais en plus on peut lire à l'intérieur comment il procède, le corriger, l'augmenter, s'en inspirer ou simplement le recopier dans un chapitre d'un autre livre.

Les premiers programmes écrits par le mouvement OSS étaient plutôt destinés aux informaticiens. Ces premières réussites ont permis de construire des équipes, de définir des modes d'organisation et de fournir les bases des programmes à venir. Elles ont permis l'émergence de programmes destinés cette fois aussi bien au grand public qu'aux informaticiens. Vous avez peut-être déjà entendu parler de certains d'entre eux, comme Linux, Gimp ou OpenOffice. Si ce n'est pas le cas, patientez encore un peu : vous ne tarderez pas à les voir apparaître dans la presse, puis sur votre ordinateur. Nous sommes à l'aube d'une mutation profonde de l'informatique, dans laquelle l'amour du travail bien fait conquerra la place qu'il mérite. Le gagnant de cette révolution, c'est vous.

Lorsque votre curiosité vous a poussé à vous documenter sur Firefox, vous vouliez peut-être seulement échapper aux failles de sécurité d'Internet Explorer. Vous avez bénéficié au passage de fonctionnalités innovantes dont vous ne pourrez bientôt plus vous passer. Et vous voilà devenu acteur d'une révolution. Firefox vous réserve encore d'excellentes surprises. Découvrons-les maintenant ensemble.