



G Data

Whitepaper 09/2010

Quels dangers de sécurité pour les joueurs ?

Sabrina Berkenkopf, Ralf Benz Müller & Marc A. Ester
G Data SecurityLabs

Go Safe. Go Safer. **G Data.**



Table des matières

Introduction	2
Types d'attaques	3
Hameçonnage par email	3
Hameçonnage sur site Web	3
Hameçonnage dans les forums et les chats.....	3
Les autres scénarios possibles	4
Familles de parasites – comportement et activité	5
Sites Internet de jeux infectés.....	6
Le marché noir	8
Plateformes de vente	9
Protection contre les attaques et la fraude	10

Introduction

L'industrie du divertissement a le vent en poupe et les jeux informatiques constituent toujours une grande proportion des chiffres de vente de la branche.

En 2009, selon l'Interactive Software Federation of Europe (www.isfe-eu.org), 253 millions de jeux pour une valeur totale de 8 milliards d'euros ont été vendus dans le commerce de détail en Europe de l'Ouest. Toujours selon l'ASFE, environ 25 % des adultes européens jouent à des jeux numériques. Si la diversité des plateformes de jeux s'accroît, le PC reste néanmoins le support le plus fréquemment utilisé. Parmi les personnes interrogées par l'ISFE, un joueur sur deux a cité l'ordinateur comme plate-forme favorite. Aux États-Unis, plus de 85 % des joueurs en ligne ont indiqué lors d'une étude, utiliser l'ordinateur pour jouer¹.

L'offre de jeux gratuits dans les réseaux sociaux s'accroît également sans cesse. Le partenariat récemment conclu entre le développeur de jeux Zynga et Facebook conduira à une augmentation considérable du nombre de jeux. D'une manière plus générale, les jeux sur navigateur s'imposeront de plus en plus à l'avenir avec un poids commercial croissant. Une situation suscitera à terme l'intérêt des cybercriminels.

À l'heure actuelle, l'activité principale des cybercriminels se concentre sur les jeux établis sur PC. World of Warcraft et les autres jeux, communément appelés massivement multijoueurs (MMORPGs), en sont des exemples représentatifs. Comptes et produits in-game atteignent sur des plateformes de vente spécialisées des tarifs pouvant atteindre plusieurs milliers d'euros. Ces sommes incitent naturellement les cybercriminels à voler les données d'accès des joueurs en ligne.

¹ Analyse de The NPD Group, inc. - http://www.npd.com/press/releases/press_100302.html

Types d'attaques

Les cybercriminels tentent sous les formes les plus diverses d'accéder aux données d'accès des joueurs. À cet effet, ils disposent d'un arsenal de solutions illégales : emails et pages Internet falsifiés ou encore programmes espions à installer sur l'ordinateur des victimes.

Hameçonnage par email

L'inspiration des fraudeurs ne connaît ici quasiment aucune limite. Voici une astuce appréciée des malfaiteurs : ils envoient des millions de spams à des joueurs en ligne potentiels. Ils falsifient fréquemment l'expéditeur et l'adresse d'expédition, et imitent ainsi les éditeurs de jeux. Voici quelques exemples de lignes d'objet de faux email, utilisés dans le cadre du jeu World of Warcraft :

- Blizzard Notification About World of Warcraft Account
- FREE Games gold Warcraft
- WorldofWarcraft mounts Trial notice
- World of Warcraft Account Security Verification
- World of Warcraft Account – Subscription Change Notice
- World of Warcraft – Account Instructions
- World of Warcraft – Account warning

Alarmants ou aguichants, ces titres n'ont d'autres finalités que de pousser les joueurs à communiquer leurs données d'accès de jeu en ligne. De faux sites Web sont ainsi créés à cet effet. Une autre méthode consiste à inviter les joueurs à télécharger un fichier joint à l'email (fichier .exe, fichier .pdf, etc.). Ce fichier est censé contenir par exemple un patch, une mise à niveau, une facture ou un formulaire d'inscription. Une fois exécuté/ouvert, ce fichier infecte l'ordinateur.

Hameçonnage sur site Web

Une autre possibilité pour récolter des données de joueurs consiste à créer de vrais faux sites Internet. Les cybercriminels copient simplement le code source de la page Web d'origine et le mettent en ligne sur leur propre serveur. Ces sites sont ensuite référencés dans les moteurs de recherche et attendent leurs victimes potentielles.

Il existe aussi des sites Web à la structure visuelle et technique très simple qui promettent aux visiteurs des pièces d'or supplémentaires, des crédits, ou des objets spéciaux pour le jeu en ligne. Tout joueur entrant ses données d'accès dans l'espoir d'obtenir des bonus perd la totalité de son compte au profit du malfaiteur. Plus d'informations à ce sujet au chapitre « Sites Internet de jeux infectés ».



Screenshot 1: Une page d'hameçonnage attrayante qui promet de soi-disant bonus

Hameçonnage dans les forums et les chats

Une autre astuce employée par les malfaiteurs consiste à se faire passer dans les forums ou les chats pour le support technique des éditeurs de jeux. Sur ces endroits d'échange, les joueurs qui rencontrent des problèmes dans le jeu sont invités à communiquer leur identifiant à ce faux service technique afin de pouvoir les dépanner. Les débutants notamment, appelés Newbies, sont les cibles privilégiées de ces attaques.

Les autres scénarios possibles

Les joueurs peuvent perdre leurs données importantes de nombreuses autres manières. Les programmes malveillants peuvent eux aussi récolter les données des joueurs. Ces dangers peuvent se dissimuler dans des copies (illégales) de jeux connus ou encore des générateurs de clés. Une fois installés, ces programmes malveillants sont à l'affût de différentes données et peuvent les obtenir des manières suivantes :

Clé de licence des logiciels

Les clés de licence des logiciels sont consignées à différents endroits de l'ordinateur. Il s'agit souvent de clés définies dans le registre, mais elles peuvent aussi être stockées dans des fichiers plus ou moins cachés situés à des endroits déterminés. Des endroits connus par les logiciels pirates. Ces données dérobées sont ensuite communiquées à des serveurs qui contrôlés par les cybercriminels.

Mots de passe dans le navigateur

Tous les navigateurs courants proposent les fonctions permettant de sauvegarder les mots de passe et les données de formulaire. Cette fonction extrêmement pratique et confortable facilite énormément l'utilisation des mots de passe. Elle possède cependant un inconvénient : les données sont stockées dans l'ordinateur à un endroit connu de tous. La protection des mots de passe étant de plus insuffisante, les dérobeurs de mot de passe peuvent facilement les identifier et les voler. Certains navigateurs ou plug-ins de navigateurs proposent des fonctions de codage, qui rendent alors des données dérobées inutiles, dès lors que le codage a lieu à l'aide d'un mot de passe suffisamment long. Certains programmes malveillants utilisent donc les données là où elles sont à nouveau décryptées : dans les champs de formulaire des sites Web correspondants. De tels « Form grabber » peuvent également lire les contenus de champs de mot de passe et les transmettre aux serveurs des usurpateurs de données.

Enregistreur de frappe

Certains programmes malveillants peuvent également enregistrer les activités du clavier. De tels programmes sont appelés des enregistreurs de frappe (keylogger). Cependant, cette désignation est dans de nombreux cas trop restrictive, car les enregistreurs de frappe peuvent enregistrer bien davantage. La plupart d'entre eux surveillent le presse-papiers et enregistrent tout ce qui est copié dans celui-ci. De nombreux enregistreurs de frappe font des captures d'écran régulières de l'ensemble de l'écran (screenlogger) ou enregistrent lors d'un clic de souris la partie de l'écran autour du pointeur de la souris. Dans bon nombre de cas, les enregistrements sont liés à des conditions, comme la visite d'un site Web particulier,

la présence de formulaire Web, l'exécution de certains jeux ou autres logiciels. Souvent, les enregistreurs de frappe utilisés travaillent de manière omnidirectionnelle, ce qui signifie qu'ils dérobent bien plus que les mots de passe des jeux. Dans de nombreux cas, les victimes des enregistreurs de frappe perdent l'accès à leur compte e-mail, à des forums, des magasins en ligne et des réseaux sociaux – en résumé: tout ce qui constitue leur identité en ligne.

Attaque par dictionnaire et par force brute

Les données d'accès aux comptes de jeux, forums, etc. peuvent également être obtenues via des essais multiples. Pour cela, les auteurs d'attaques utilisent de longues listes de mots de passe fréquents (attaque par dictionnaire) ou combinent des lettres au hasard et des suites de chiffres jusqu'à une certaine longueur (attaque par force brute). Ceux qui utilisent des mots de passe courants ou courts comme « 123456 », « Admin », ou « Master » sont des victimes potentielles.

Familles de parasites – comportement et activité

Les programmes malveillants peuvent être détectés sur la base de certaines propriétés dans leur code. À l'aide de similitudes dans le code de programme de différents parasites, chaque variante de parasites peut être regroupée en familles. Les familles les plus fréquentes dans le domaine du jeu et leurs activités typiques sont décrites ici :

OnlineGames

OnlineGames est la famille la plus fréquente. Ses variantes constituent 1,9 % de tous les parasites au cours du premier semestre 2010 et elle occupe la 7^e place des familles les plus productives. OnlineGames compte parmi le groupe des dérobeurs de mot de passe. Ce groupe réunit les parasites qui ne se limitent pas aux simples jeux. La liste des jeux attaqués est longue et contient entre autres les jeux suivants :

<i>2moons</i>	<i>Fly for fun</i>	<i>Maple Story</i>	<i>Online</i>
Age of Conan	Gash	Metin 2	Twelve Sky
Aion Online	Goodluck	Perfect World	Valhalla
Cabal Online	Knight Online	Seal Online.	World of Warcraft
Dekaron	Last Chaos	Silk Road Online	
Dungeon Fighter	Lineage	The Lord of the Rings	

Pour se cacher, les parasites de cette famille intègrent leurs fonctions nuisibles à l'Explorateur Windows. Certains dissimulent leurs fichiers et entrées de registre également via des pilotes Rootkits. Pour pouvoir agir en toute liberté, les outils antipiratage d'éditeurs de jeux comme HShield ou GameGuard sont contournés. La plupart des variantes de OnlineGames se copient sur tous les partages et s'y inscrivent dans un fichier autorun.inf. De cette manière, ils sont activés automatiquement lorsqu'une clé USB ou un autre support de données amovibles est raccordé.

Magania

Cette famille de parasites est principalement active en Asie orientale. Avec une proportion de 1,6 % du volume total de parasites du premier semestre 2010, elle occupe la 11^e place des familles de parasites les plus productives. Magania fait partie du groupe des enregistreurs de frappe et vise les jeux comme Lineage ou MapleStory. Dans la plupart des cas, les parasites surviennent par email. Si la pièce jointe au fichier est exécutée, une image de diversion est affichée. Le parasite est actif en arrière-plan. Pour se cacher, les parasites de la famille Magania intègrent les processus de l'Explorer et d'Internet Explorer et sont ainsi invisibles pour l'utilisateur. Les données d'accès dérobées sont transmises sur plusieurs serveurs distants. D'autres programmes malveillants de différentes natures sont fréquemment téléchargés.

WOW

Les parasites de la famille « WOW » convoitent les données d'accès de World of Warcraft. Avec une proportion de 0,3 % au cours du premier semestre 2010, il se placent au 49^e rang. Ils sont ainsi la plus grande famille ayant convoité un seul jeu. Les données sont dérobées par enregistrement de frappe et transmises à des serveurs sur Internet. Les données d'accès dérobées sont utilisées pour usurper les comptes des victimes et vendre les personnages et biens virtuels dans des forums spécialisés.

Autres familles

La famille « Lmir » occupe la 75^e place des familles de parasites les plus productives du premier semestre 2010. Ses représentants ont convoité les données d'accès au jeu « Legend of Mir », très populaire en particulier en Chine et en Corée du Sud. Au rang 103 se place Tibia, une famille d'enregistreurs de frappe, ayant convoité les données d'accès du jeu allemand du même nom.

Sites Internet de jeux infectés

Une étude menée par le G Data SecurityLabs sur 66.534 pages Web recensées comme dangereuses (Sites d’hameçonnage ou infectés) entre le 1er janvier 2010 et le 30 juin 2010 montre que 6,5 % de ces pages traitent du jeu vidéo. Sur cet échantillon, la répartition se décompose comme ceci :

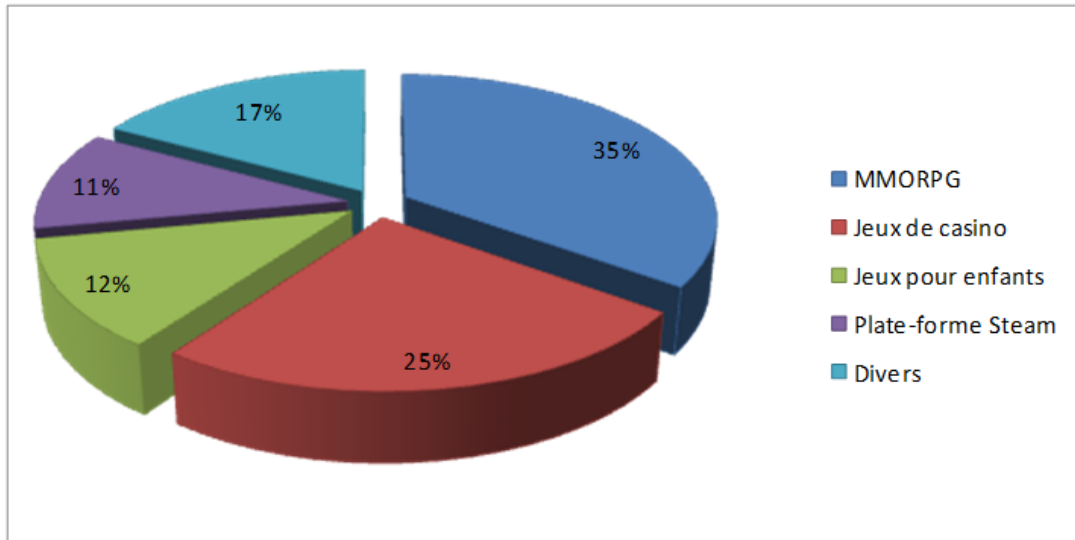
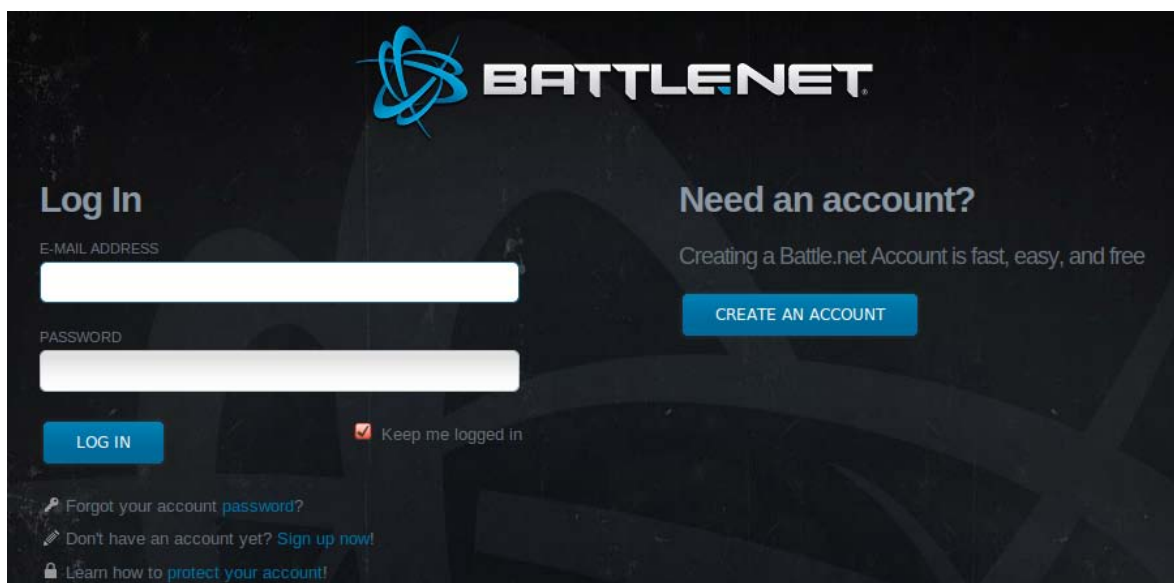


Diagramme 1: Pourcentage des différents thèmes des pages de jeux étudiées

Les jeux de rôle de masse en ligne occupent clairement la première place, avec une proportion de 35 % : des jeux comme World of Warcraft, Metin 2, Runescape, Tibia et autres en font partie. Le scénario d’attaque enregistré le plus fréquemment par G Data est l’hameçonnage. Les fraudeurs imitent la page Web de connexion d’origine des jeux en question, la placent en ligne sur leur propre serveur. Une page qui est d’un point de vue graphique et typographique difficile à différencier de l’originale.



Capture d’écran 2: Un extrait d’une fausse page de connexion, impossible à différencier visuellement de l’originale

Original (USA)	https://us.battle.net/login/en/
Exemples de falsifications	http://us.bvttie.net/login/login.htm http://us.bottlo.net/login/login.xmlref.html http://us-battlefusbattlenet.net http://us-battletests.net http://us.bbattlie.net http://us.balittlie.com http://www.account-battle.net/wow http://www.wowsupport.net

Tableau 1: Similitudes typographiques des adresses Web des pages d’hameçonnage Battle.net par rapport au site d’origine

Dans le domaine des jeux de casino (le poker principalement) et les jeux pour enfants (souvent des communautés virtuelles), les fraudeurs tentent d’usurper les comptes avec de soi-disant pages de bonus.

Les comptes de la plateforme Steam sont particulièrement convoités, car les joueurs peuvent y utiliser plusieurs jeux à l’intérieur d’un seul compte et les escrocs accèdent ainsi via l’hameçonnage pas seulement à un jeu, mais dans certains cas à plusieurs. Ces données d’accès Steam sont ensuite vendues entre autres au marché noir (voir tableau 2).

Le marché noir

N’importe quel produit ou presque est vendu sur les marchés noirs en ligne – des comptes de différents services de paiement et de services de vente aux enchères en ligne, aux données d’accès et clés pour des programmes et des jeux, en passant par des cartes d’identité et des données de cartes de crédit. Les prix indiqués sont des exemples issus de plateformes commerciales illégales :

Steam & Battle.net Accounts	Prix
Counter-Strike 1.6, Counter-Strike : Source, Counter-Strike : Condition Zero, Day of Defeat, Day of Defeat : Source, Half-Life, Half-Life Deathmatch Classic, Half-Life Opposing Force, Half-Life Blue Shift, Half-Life 2, Half-Life 2 Deathmatch, Half-Life 2 Lost Coast, Red Orchestra : Ostfront 41-45, Ricochet, Saints Row 2, Speedball 2 Tournament, Team Fortress Classic	40 euros
Counter-Strike : Source, Dark Messiah of Might & Magic, Day of Defeat : Source, Left 4 Dead, Left 4 Dead 2, Metro 2033, Saints Row 2, Supreme Commander	35 euros
Call of Duty : Modern Warfare 2 Uncut	22 euros
Counter-Strike : Source, Counter-Strike 1.6, Half-Life 2 Episode 1 et 2, Team Fortress 2	20 euros
Call of Duty : Modern Warfare 2, Order of War, Order of War Challenge	20 euros
Counter-Strike : Source, Day of Defeat : Source, Half-Life 2 Lost Coast, Half-Life 2 Deathmatch	16 euros
Alien vs. Predator Uncut	12 euros
Starcraft II : Wings of Liberty, World of Warcraft	10 euros
Empire : Total War, Warhammer 40,000 Dawn of War II, Warhammer 40,000 : Dawn of War II Chaos Rising	10 euros

GRID	5 euros
Trackmania United Forever, Tombraider : Underworld	5 euros
Counter-Strike 1.6	5 euros

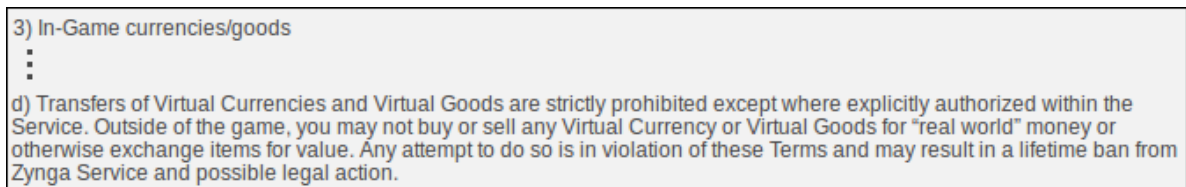
Gamekeys	Prix
Battlefield : Bad Company 2 – Limited Edition	15 euros
Assassin’s Creed – Special Edition	12 euros
Command & Conquer 4 : Tiberian Twilight	12 euros
World of Warcraft Wrath of the Lich King – Collector’s Edition	12 euros
World of Warcraft Wrath of the Lich King	10 euros
Aion	10 euros
Battlefield : Bad Company 2	10 euros
FIFA 10	9 euros
World of Warcraft Burning Crusade	6 euros
World of Warcraft Classic	5 euros

Gametime & Points	Prix
Playstation Network Card (50,00 euros)	18 euros
Carte d'abonnement Or de 12 mois à Xbox Live	12 euros
World of Warcraft Gametime 60 jours	10 euros
NCSOFT Gametime 60 jours	10 euros
1.000 points Sim	8 euros
1 000 points Wii	5 euros

Tableau 2: Sélection de prix pour les produits de jeux issus de quelques boutiques souterraines




Plateformes de vente

Les biens et comptes virtuels sont vendus sur d’autres plateformes, plus ou moins légales. À côté des services de ventes aux enchères mondialement connus cohabitent des services spécialement dédiés ou seuls des produits In-Game et des données d’accès sont vendus. playerauctions.com, mmobay.net ou encore wowbay.net en sont quelques exemples. Notez que le vendeur et l’acheteur d’articles de jeux et de comptes en dehors de l’environnement du jeu enfreignent les conditions d’utilisation de la plupart des éditeurs de jeux, comme Blizzard, Zynga, etc.



Capture d’écran 3: Extrait issu des conditions d’utilisation de Zynga, illustrant l’interdiction

Exemple : Sur le service de vente aux enchères playerauctions.com, des comptes de haute valeur sont proposés à des prix très élevés. Le prix s’oriente en fonction du niveau du personnage, des capacités, des objets virtuels disponibles et du serveur sur lequel joue ce personnage. Si l’offre la plus faible remarquée sur ce site comprend 29 comptes pour 40 dollars, la capture d’écran ci-dessous montre que des prix bien plus élevés peuvent être atteints.

Offer	Price ▲	Seller's Delivery Guarantee ?	Date	Secure Payment
 Superior WoW account - Offering: Mage + Rogue + DK tank/DPS 6420 GS ++ all of em and include SC2	\$2,550.00	24 Hours	Aug-06	View Details
Ashes of Al'ar mount and full t10 Tank/Kitty/Tree and pvp gear sets!	\$2,212.00	24 Hours	Jul-28	View Details
 Level 80 lock gnome alliance 3900 SP 6190 GS pve and 6075 GS pvp 11/12 ICC25 heroic + 5 lvl 80 toons	\$1,100.00	24 Hours	Aug-08	View Details
 2xLVL 80 Kingslayer Account + Everything you would ever want	\$800.00	20 Minutes	Aug-08	View Details
80 Orc hunter 6k gs & 80 Troll shaman 6k gs. 12/12 in both 10/25man and 11/12 HM achievement.	\$670.00	24 Hours	Jul-26	View Details

Capture d'écran 4: Les comptes actuellement les plus chers chez playerauctions.com

De tels chiffres montrent pourquoi les joueurs sont dans la ligne de mire des cybercriminels. Il ne s'agit pas seulement de loisir, de plaisir et de pièces en or virtuelles, mais bel et bien de réelle valeur monétaire !

Protection contre les attaques et la fraude

Afin de jouer en toute quiétude, les conseils et astuces suivants doivent être respectés :

- Un logiciel de sécurité intégrant un filtre HTTP, un pare-feu et une fonction de surveillance comportementale doit être installé et actif pour protéger l'ordinateur contre les logiciels espions et autres menaces.
- Un filtre antispam permet de trier les e-mails indésirables avant qu'ils n'atterrissent dans la boîte de réception.
- La protection des comptes de jeu par un mot de passe complexe est très importante. Une combinaison de 8 caractères au minimum, composée de chiffres en majuscules et minuscules et de caractères spéciaux doit être idéalement utilisée.
- Un mot de passe différent doit être configuré pour chaque compte et les mots de passe ne doivent pas être enregistrés dans le navigateur. Pour se rappeler les nombreux mots de passe, il est possible de les composer d'une partie fixe et d'une partie variable.
- Les attaques par hameçonnage sur des joueurs en ligne sont souvent sophistiquées. Mais en regardant d'un peu plus près la ligne d'adresse du navigateur, il est possible de se rendre compte dans la plupart des cas s'il s'agit d'une fausse page Internet.