Les menaces informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en oeuvre des dispositions préventives.

Les menaces informatiques

Motivation des attaques

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- glaner des informations personnelles sur un utilisateur
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- troubler le bon fonctionnement d'un service
- utiliser le système de l'utilisateur comme « rebond » pour une attaque
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

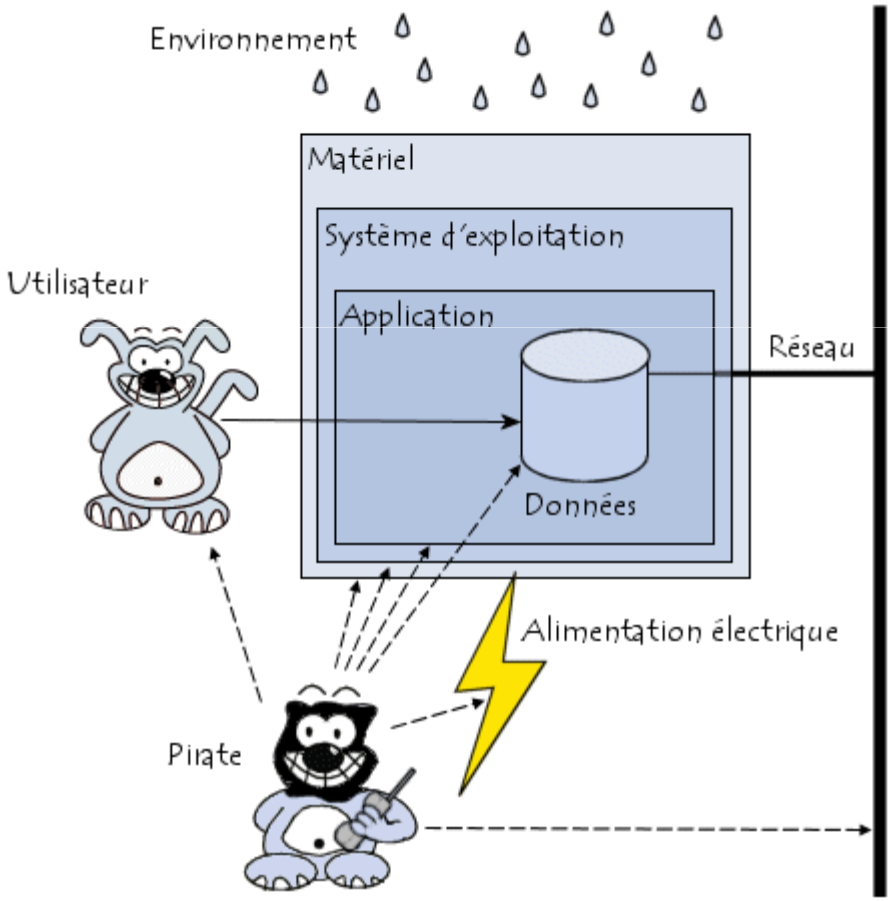
Les menaces informatiques

Motivation des attaques

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.

Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable.

Le schéma ci-dessous rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :



Les menaces informatiques

L’attaque par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux **attaques directes**), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.
Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

Les menaces informatiques

Les différentes attaques

Accès physique : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

- Coupure de l'électricité
- Extinction manuelle de l'ordinateur
- Vandalisme
- Ouverture du boîtier de l'ordinateur et vol de disque dur
- Ecoute du trafic sur le réseau

- **Interception de communications** :
- Vol de session (*session hijacking*)
- Usurpation d'identité
- Détournement ou altération de messages

Les menaces informatiques

Les différentes attaques : Déni de service

Une « **attaque par déni de service** » (en anglais « **Denial of Service** », abrégé en *DoS*) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information.

La plupart des attaques par déni de service exploitent des failles liées à l'implémentation d'un protocole du modèle TCP/IP.

Les menaces informatiques

Les différentes attaques : Déni de service

On distingue habituellement deux types de dénis de service :

• Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles
• Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Le principe des attaques par déni de service consiste à envoyer des paquets IP afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « **déni de service distribué** » (noté *DDOS* pour *Distributed Denial of Service*). Les attaques par déni de service distribué les plus connues sont *Tribal Flood Network* (notée *TFN*).

Se protéger d'un déni de service
Pour se protéger de ce type d'attaque, il est nécessaire de récupérer sur internet des correctifs logiciels (patchs) http://windowsupdate.microsoft.com/

Les menaces informatiques

Les différentes attaques – IP Spoofing

L'usurpation d'adresse IP

L'« **usurpation d'adresse IP** » (également appelé *mystification* ou en anglais *spoofing IP*) est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine.

Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement.

Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une *mascarade* de l'adresse IP au niveau des paquets émis.

En effet, un système pare-feu (en anglais *firewall*) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau. L'usurpation d'IP permet de contourner le mur de feu.

Les menaces informatiques

Contre mesure – Le firewall

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique.

La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.
Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons :

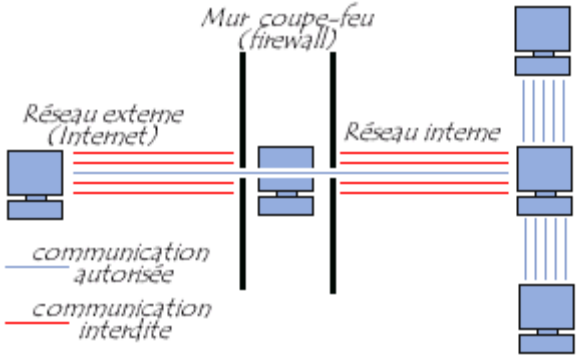
- La machine cible est susceptible d'être connectée sans pour autant être surveillée
- La machine cible est généralement connectée avec une plus large bande passante
- La machine cible ne change pas (ou peu) d'adresse IP

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection.

Les menaces informatiques

Contre mesure – Le firewall

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :
une interface pour le réseau à protéger (réseau interne) ;
une interface pour le réseau externe.



Le système firewall est un système logiciel

Les menaces informatiques

Contre mesure – Le firewall

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

L'ensemble de ces règles permet de mettre en oeuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées :

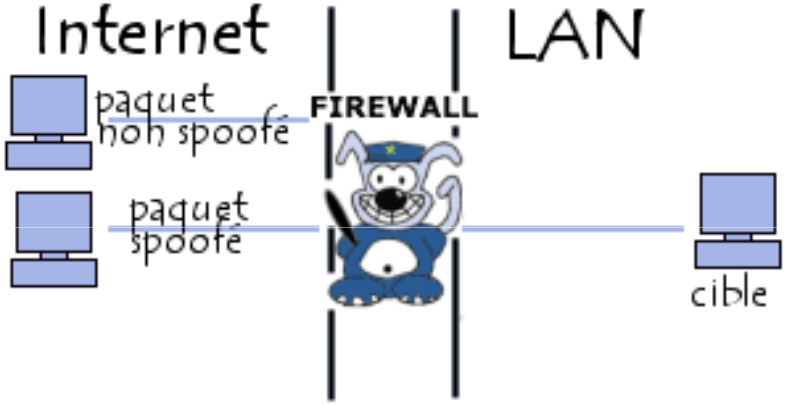
"Tout ce qui n'est pas explicitement autorisé est interdit".

- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Les menaces informatiques

Les différentes attaques – IP Spoofing



Ainsi, un paquet spoofé avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu.

Les menaces informatiques

Les différentes attaques – ARP Poisoning

Une des attaques les plus célèbres consiste à exploiter une faiblesse du protocole ARP (*Address Resolution Protocol*) dont l'objectif est de permettre de retrouver l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.

L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet falsifié indiquant que l'adresse MAC de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant.

De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice.

Les menaces informatiques

Les différentes attaques – Les analyseurs réseau (sniffer)

Un « **analyseur réseau** » (en anglais *sniffer*, traduisez « renifleur ») est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.

En effet, dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Toutefois, dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Ainsi, en utilisant l'interface réseau dans un mode spécifiqueil est possible d'écouter tout le trafic passant par un adaptateur réseau (une carte réseau ethernet, une carte réseau sans fil, etc.).

Ex: écoute du port spécifique de messenger ;)

Parade:

- utilisation de protocole de cryptage des données (chiffrage)
- Utiliser un détecteur de sniffer.
- Pour les réseaux sans fils il est conseillé de réduire la puissance des matériels de telle façon à ne couvrir que la surface nécessaire. Cela n'empêche pas les éventuels pirates d'écouter le réseau mais réduit le périmètre géographique dans lequel ils ont la possibilité de le faire.

Les menaces informatiques

Les différentes attaques – Balayage des ports

Un « **scanner de vulnérabilité** » (parfois appelé « *analyseur de réseaux* ») est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts (en anglais *port scanning*) sur une machine donnée ou sur un réseau tout entier. Le balayage se fait grâce à des sondes (requêtes) permettant de déterminer les services fonctionnant sur un hôte distant.

Un tel outil permet de déterminer les risques en matière de sécurité. Il est généralement possible avec ce type d'outil de lancer une analyse sur une plage ou une liste d'adresses IP afin de cartographier entièrement un réseau.

Un scanner de vulnérabilité est capable de déterminer les ports ouverts sur un système en envoyant des requêtes successives sur les différents ports et analyse les réponses afin de déterminer lesquels sont actifs.
En analysant très finement la structure des paquets TCP/IP reçus, les scanners de sécurité évolués sont parfois capables de déterminer le système d'exploitation de la machine distante ainsi que les versions des applications associées aux ports et, le cas échéant, de conseiller les mises à jour nécessaires, on parle ainsi de caractérisation de version.

Les menaces informatiques

Les différentes attaques – Vulnérabilité des serveurs Web

Le protocole HTTP (ou HTTPS) est le standard permettant de véhiculer les pages web par un mécanisme de requêtes et de réponses. Utilisé essentiellement pour transporter des pages web informationnelles (pages web statiques), le web est rapidement devenu un support interactif permettant de fournir des services en ligne.

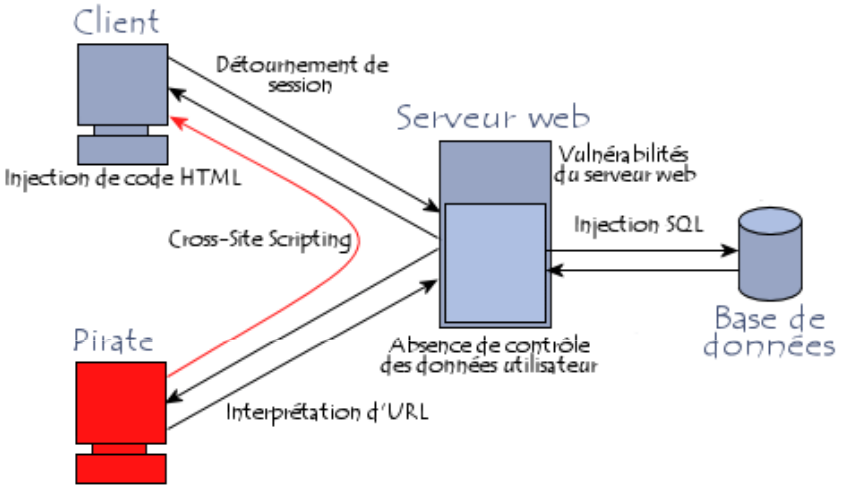
Le terme d'« application web » désigne ainsi toute application dont l'interface est accessible à travers le web à l'aide d'un simple navigateur. Devenu le support d'un certain nombre de technologies le protocole HTTP possède désormais un rôle stratégique certain dans la sécurité des systèmes d'information.

Dans la mesure où les serveurs web sont de plus en plus sécurisés, les attaques se sont progressivement décalées vers l'exploitation des failles des applications web.

Ainsi, la sécurité des services web doit être un élément pris en compte dès leur conception et leur développement.

Les menaces informatiques

Les différentes attaques – Vulnérabilité des serveurs Web



Parade: Le principe de base à retenir d'une manière générale lors de tout développement informatique est qu'il ne faut pas faire confiance aux données envoyées par le client.

Utilisation de **cookies**

Conséquences: Les attaques à l'encontre des applications web sont toujours nuisibles car elles donnent une mauvaise image de l'entreprise. Les conséquences d'une attaque réussie peuvent notamment être une des suivantes :

- Effacement de site web
- Vol d'informations
- Modification de données, notamment modification de données personnelles
- Intrusion sur le serveur web

Les menaces informatiques

Les cookies

Quels sont ces étranges gateaux qu'un site web vous a sûrement déjà proposé?

La plupart du temps, lorsqu'un serveur web propose un cookie, les utilisateurs ignorent ce terme et cliquent sur « OK;» sans se préoccuper de son devenir. Un **cookie** est en réalité un fichier stocké sur le disque dur de l'utilisateur, afin de permettre au serveur web de le reconnaître d'une page web à l'autre. Les cookies sont notamment utilisés par les sites de commerce électronique afin de conserver les préférence de l'utilisateur (par exemple les options qu'il a coché) afin de lui éviter de les ressaisir.

Le problème majeur des cookies relève des informations qu'ils contiennent. En effet, lorsqu'un utilisateur se connecte à un site personnalisable, celui-ci va lui poser quelques questions afin de dresser son profil, puis stocker ces données dans un cookie.
Selon le site, la manière de laquelle l'information est stocké peut s'avérer nuisible à l'utilisateur. En effet, un site de vente en ligne peut par exemple collecter des informations sur les préférences des utilisateurs par le biais d'un questionnaire, afin de leur proposer ultérieurement des articles pouvant les intéresser.

Les menaces informatiques

Les cookies

Un cookie est ainsi un mécanisme prévu pour créer une association entre la session de l'utilisateur (navigation entre des pages d'un même site pendant une période donnée) et les données le concernant.
Idéalement, le cookie doit contenir une chaîne aléatoire (identifiant de session) unique et difficilement devinable, valide uniquement pendant un temps donné. Seul le serveur doit pouvoir être en mesure d'associer les préférences de l'utilisateur à cet identifiant.
En aucun cas le cookie ne doit contenir directement les informations concernant l'utilisateur et sa durée de vie doit être la plus proche possible de celle correspondant à la session de l'utilisateur.
D'autre part, les données stockées dans un cookie sont envoyées par le serveur, sur la base des données renseignées par l'utilisateur. Ainsi, le cookie ne peut en aucun cas contenir des informations sur l'utilisateur qu'il n'a pas données ou d'information sur le contenu de l'ordinateur, ou en d'autres termes: le cookie ne peut pas collecter d'informations sur le système de l'utilisateur.
Ainsi, refusez de céder des informations personnelles à un site ne vous inspirant pas confiance car il n'a aucune raison de collecter des informations vous concernant.
Un cookie n'a donc rien de dangereux en soi s'il est bien conçu et si l'utilisateur ne donne pas d'informations personnelles.

Les menaces informatiques

Les différentes attaques – Le Pishing

Le **phishing** (contraction des mots anglais « *fishing* », en français *pêche*, et « *phreaking* », désignant le *piratage de lignes téléphoniques*), traduit parfois en « **hameçonnage** », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Les menaces informatiques

Les différentes attaques – Le Pishing

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.

Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).

Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

Les menaces informatiques

Les différentes attaques – Le Pishing

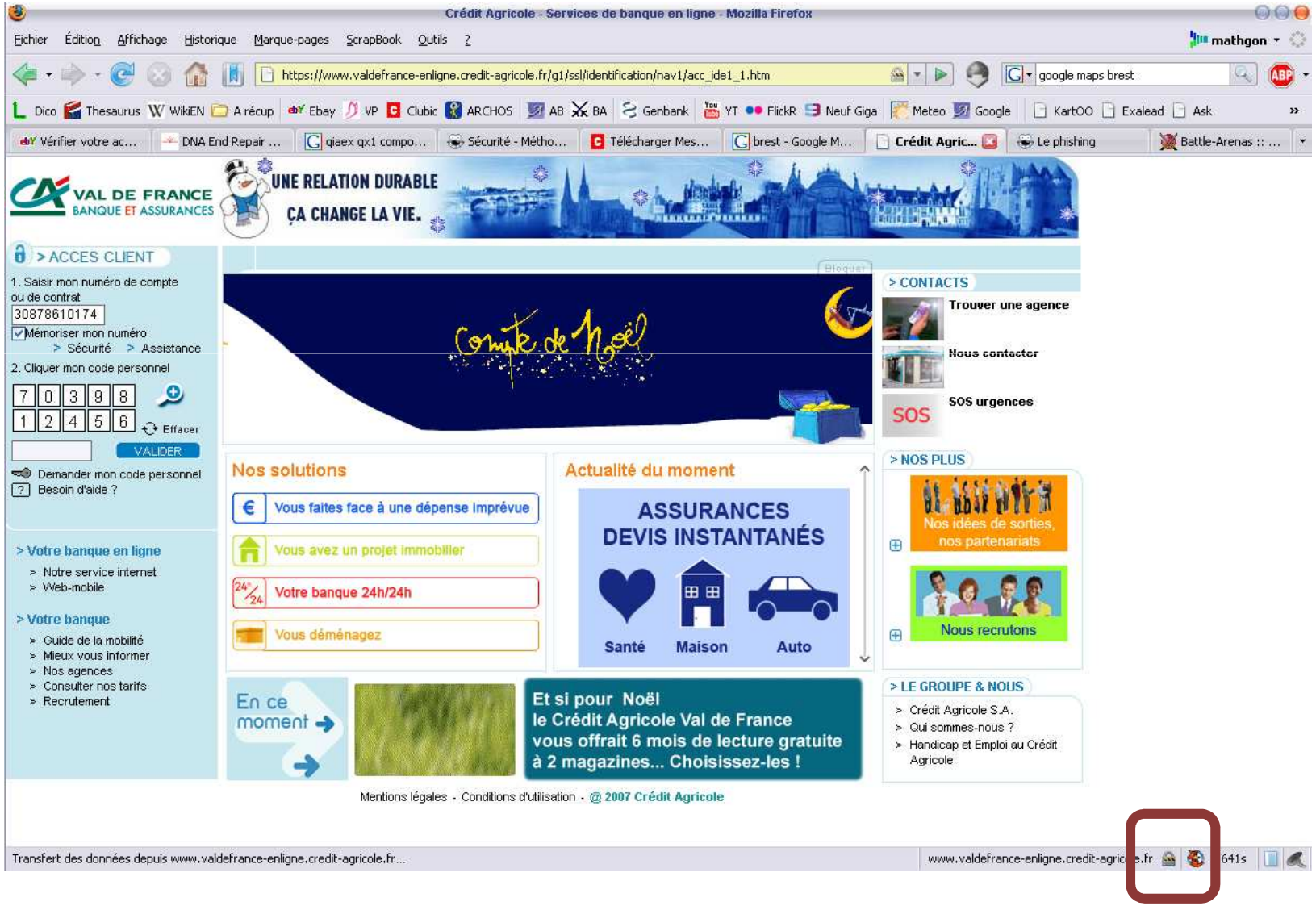
Parades:

•Ne cliquez pas directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'URL d'accès au service.

•Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par *https* et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse correspond bien à celui annoncé (gare à l'orthographe du domaine) !

Les menaces informatiques

Les différentes attaques – Le Pishing



Les menaces informatiques

Les différentes attaques – Les trappes

il s'agit d'une porte dérobée (en anglais *backdoor*) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.