République Algérienne Démocratique & Populaire

PUBLICITÉS MALVEILLANTES

comment se prémunir?

GUIDE POUR

- *Les utilisateurs*
- *Les Responsables de la Sécurité des Systèmes d'Information*
- *Les développeurs*

Publicités malveillantes: *comment se prémunir?*

INTRODUCTION

Internet est devenu un moyen de communication d'une grande portée et à fort potentiel pour les experts en marketing. L'espace cyber est devenu l'un des marchés les plus importants pour la publicité. Les fournisseurs de la publicité exploitent le web pour la diffusion de leurs contenus sous plusieurs formes, notamment les bannières publicitaires insérées sur les pages électroniques.
Avec l'émergence de la publicité en ligne, les cybercriminels exploitent particulièrement cette dernière, souvent diffusée à grande échelle, pour réussir leurs cyberattaques sur des personnes ciblées et non ciblées.
Ce guide contient un ensemble de recommandations de bonnes pratiques destinées aux utilisateurs, développeurs et responsables de la sécurité des systèmes d'information, permettant la prévention et la protection contre le phénomène des publicités malveillantes.

*Que sont les **publicités malveillantes** (Malvertising) ?*

Le phénomène des publicités malveillantes, appelé (Malvertising), consiste à injecter un code malveillant dans les publicités numériques. Ces publicités infectées sont généralement diffusées aux consommateurs à travers des réseaux publicitaires et des sites web de confiance. Ces publicités risquent d'infecter votre appareil avec ces codes malveillants, même si vous ne cliquez pas dessus.

*Comment peuvent-elles **vous infecter**?*

L'infection par les publicités malveillantes se produit généralement de deux manières:

1.

***En cliquant sur les publicités,** qui peuvent être des fenêtres contextuelles ou des alertes d'avertissement. Les utilisateurs sont manipulés pour qu'ils installent eux-mêmes des logiciels malveillants.*

2.

***Sans cliquer,** l'utilisateur est infecté simplement en chargeant la page Web. Les publicités malveillantes contiennent des liens, intégrés dans des lignes de code permettant aux navigateurs de télécharger à l'insu des utilisateurs des logiciels à partir de pages Web malveillantes.*

La publicité malveillante constitue une atteinte aux systèmes de traitement automatisé de données et engage la responsabilité pénale de son auteur conformément à la législation en vigueur et le condamne à des peines d'emprisonnement et d'amende.

1

GUIDE

POUR LES UTILISATEURS

Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de votre navigateur Web

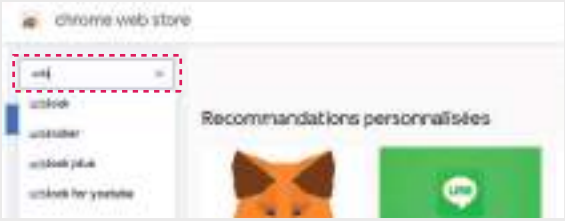
1.Installer des extensions pour bloquer le flux publicitaire:

Un bloqueur de publicité empêchera les publicités de s'afficher sur votre navigateur. Cela réduira les risques d'infection de votre appareil. Choisissez donc le bloqueur que vous souhaitez sur votre navigateur favori.

Exemple : Navigateur Chrome

Ouvrez votre navigateur Google Chrome et accédez au chrome web store.

Dans le champ recherche, saisissez le nom du bloqueur de publicités



Une fois l'extension trouvée, cliquez sur ***«Ajouter à Chrome»***

Confirmez en cliquant sur « ***Ajouter l'extension ».***

EXEMPLES DE BLOQUEURS DE PUBLICITÉS

Renforcez la sécurité de votre navigateur Web

2. Mettre à jour le navigateur Web

Il est recommandé d'activer la fonction de mise à jour automatique. Les mises à jour de sécurité sont essentielles pour garantir qu'un utilisateur est à l'abri des vulnérabilités connues.

Exemple : Navigateur Chrome

1. *Dans le coin supérieur droit de la fenêtre Chrome, cliquez sur l'icône du menu Chrome :* ⋮
2. *Dans l'élément **«Aide»**,cliquez sur **«A propos de Chrome».** Chrome déclenchera une vérification automatique des mise à jour et les installera sur votre appareil lors de leur disponibilité.*

Exemple : Navigateur Firefox

1. *Dans le coin supérieur droit de la fenêtre Mozilla, cliquez sur l'icône du menu Mozilla :* ☰
2. *Dans l'élément **«Aide»**,cliquez sur **«A propos de Mozilla».** Mozilla déclenchera une vérification automatique des mises à jour et les installera sur votre appareil lors de leur disponibilité.*

Renforcez la sécurité de votre navigateur Web

3. Gérer et paramétrer les cookies

Les cookies sont des fichiers textes stockés dans l'appareil, générés par le serveur du site-web visité. Ces fichiers contiennent les données nécessaires pour le fonctionnement du site (cookies propriétaire) et des données supplémentaires (cookies tiers). Le rôle principal des cookies est de faciliter l'utilisation ultérieure du site par le même utilisateur. Tout dépend de leur nature, certains cookies sont exploités à l'insu des utilisateurs dans des actions illicites comme la collecte des données personnelles ou les habitudes de navigation, le pistage, l'authentification et le sondage, ce qui constitue une menace à la sécurité des utilisateurs. Il est donc recommandé de n'accepter que les cookies paramétrables.

Les étapes à suivre par un utilisateur pour gérer et paramétrer les cookies :

1.Le paramétrage des cookies :

Généralement, après avoir accédé à un site-web, ce dernier demande à son visiteur d'accepter ou de refuser les cookies, voire même de paramétrer les cookies de type tiers. Dans ce cas de figure, l'utilisateur doit choisir attentivement les cookies paramétrables.

2.Le paramétrage de votre navigateur internet :

Exemple : Navigateur chrome

- Dans le coin supérieur droit de la fenêtre Chrome, cliquer sur l'icône du menu Chrome : ⋮ *et choisissez* ***«paramètres».***

- Dans la fenêtre qui s'affiche, choisissez ***« Confidentialité et sécurité»*** *puis* ***«Cookies et autres données des sites»***

- Dans la section ***« Paramètres généraux »*** *choisir* ***« Bloquer les cookies tiers ».***

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de votre navigateur Web

4. Bloquer les fenêtres pop-up

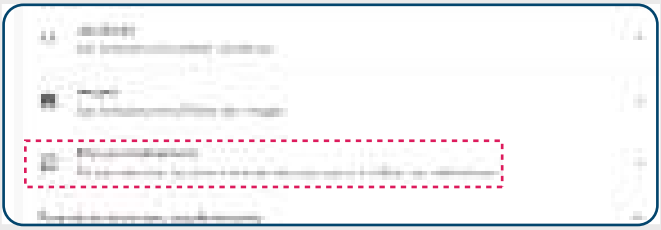
Une pop-up désigne une fenêtre qui s'affiche sur l'écran de façon automatique à l'ouverture d'une page web. Il s'agit la plupart du temps d'un message publicitaire. Ces fenêtres intrusives peuvent aussi provoquer le téléchargement masqué de fichiers malveillants. Certaines peuvent s'ouvrir automatiquement et entraîner des actions illicites, à l'insu de l'utilisateur. La majorité des navigateurs modernes comportent désormais un bloqueur de pop-up intégré qui vous permettra d'éliminer ces fenêtres.

Exemple : Navigateur Chrome

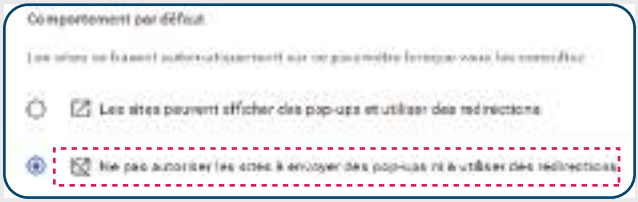
1. *- Dans le coin supérieur droit de la fenêtre Chrome, cliquez sur l'icône du menu Chrome :* ⋮ *et choisissez* ***«paramètres».***

2. *- Dans la fenêtre qui s'affiche, choisissez* ***« Confidentialité et sécurité»*** *puis* ***«paramètres des sites»***

3. *- Dans la section* ***«contenu»*** *cliquez sur* ***«Pop-up et redirections»***



4. *Dans* ***«comportement par défaut»*** *cochez* ***«Ne pas autoriser les sites à envoyer des pop-ups ni à utiliser des redirections»***



Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de votre navigateur Web

5.Apprendre à reconnaître les faux sites Web

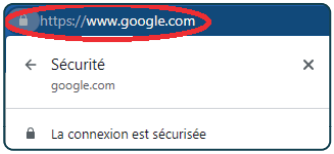
Les faux sites Web constituent un vecteur de propagation des publicités malveillantes. Il faut donc apprendre à reconnaître ce type de sites Web.

RECONNAITRE UN FAUX SITE WEB

⚠

Absence de chiffrement HTTPS

vérifier l'existence de l'acronyme https dans la barre d'adresse comme suit :



⚠

Vérifier minutieusement l'URL du site web

toute irrégularité pourrait être signe d'un faux site (ressemblance de l'URL avec des noms de sites connus, non cohérence entre l'URL et le contenu du site). ***(exemple : www.facebok.com au lieu de www.facebook.com).***

⚠

Eviter les sites proposant des offres attrayantes et trompeuses

*ou des messages du genre "**Vous êtes le visiteur N° 1000.000 Cliquez ici pour gagner un cadeau!**".*

Renforcez la sécurité de votre navigateur Web

6. Supprimer les mots de passe enregistrés dans votre navigateur

A des fins d'utilité, les utilisateurs sont nombreux à faire le choix d'accepter l'enregistrement de leurs mots de passe sur les navigateurs, une pratique qui s'avère risquée, dans la mesure où les navigateurs ne sont pas assez sécurisés pour protéger vos mots de passe. De ce fait, il est fortement recommandé de supprimer les mots de passe enregistrés dans votre navigateur et l'empêcher de les enregistrer d'une façon automatique.

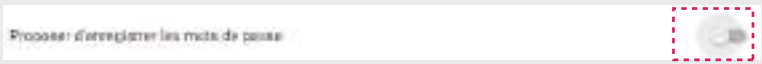
Exemple : Navigateur Chrome

1. *- Dans le coin supérieur droit de la fenêtre Chrome, cliquez sur l' Icône du menu Chrome ⋮ et choisissez* ***«paramètres».***
2. *- Dans la fenêtre qui s'affiche, choisissez* ***« Saisie automatique»*** *puis* ***«mots de passe»***

3. *- Sous la section* ***« Mots de passe enregistrés »****, supprimez un à un les mots de passe répertoriés en cliquant sur ⋮ en bout de chaque mot de passe et sélectionner* ***Supprimer.***

Pour empêcher les navigateurs d'enregistrer les mots de passe

* *Dans le menu* ***«mots de passe»*** *désactivez* ***«Proposer d'enregistrer les mots de passe»***



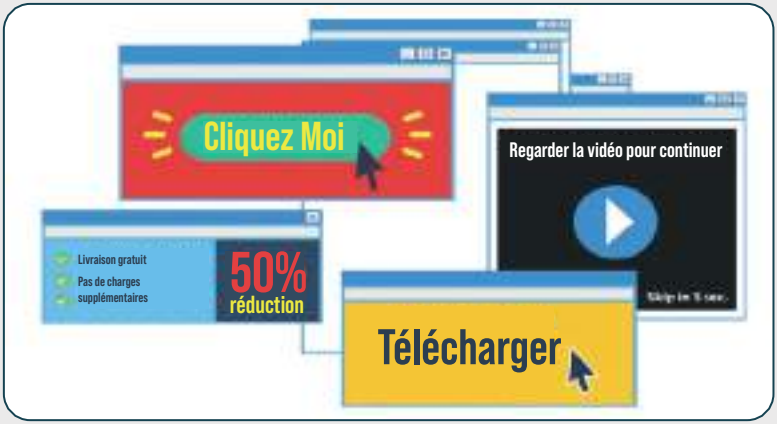
Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de votre navigateur Web

7. Eviter de cliquer sur les publicités de contenu suspect

Certaines publicités malveillantes contiennent des offres fictives. De ce fait, il est primordial avant de consulter une publicité, de s'assurer de la véracité de cette dernière à partir des sites officiels du propriétaire de l'offre.



8. Bien gérer vos mots de passe

GÉRER SES MOTS DE PASSE

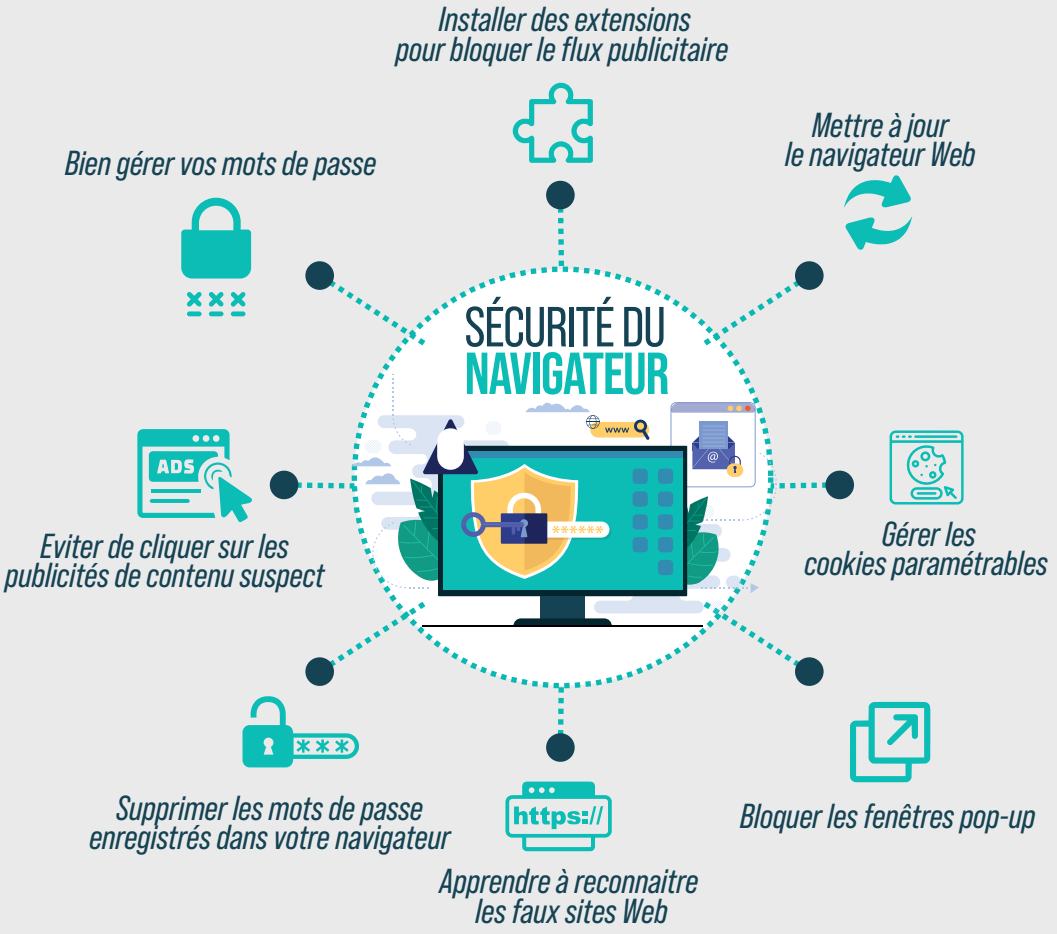
- Utilisez des mots de passe forts (long avec des lettres, des chiffres et des caractères spéciaux)
- Utilisez un mot de passe unique par compte.
- Séparez les comptes à utilisation personnelles de ceux à utilisation professionnelle.
- Utilisez l'authentification à double facteur
- Changez régulièrement les mots de passe

Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de votre navigateur Web

COMMENT SE PRÉMUNIR DES PUBLICITÉS MALVEILLANTES ?



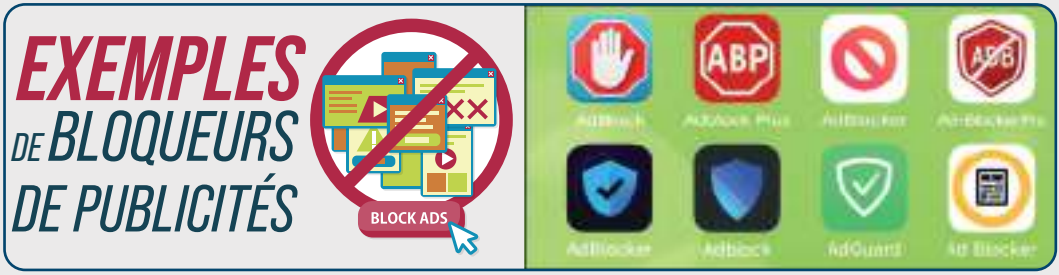
Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de vos appareils

1. Installer des applicatifs de blocage des publicités sur les appareils à protéger :

Il s'agit d'outils qui bloquent tout type d'annonce publicitaire dans les applications et les navigateurs et protègent la confidentialité des applications.
il est recommandé d'utiliser des outils en la matière, facile d'emploi et personnalisable (exemple : AdGuard). Ces outils sont disponibles en version Android et iOS pour les appareils Mobiles et Windows et MacOs pour les autres appareils.



2. Installer un antivirus professionnel tout en veillant à sa mise à jour régulière :

Il est recommandé d'installer un antivirus fiable et professionnel sur tous vos appareils avec lesquels vous vous connectez. Ces antivirus permettent d'empêcher tout acte malveillant ciblant vos appareils et de bloquer toute tentative de vol de données ou d'infection à travers les publicités malveillantes. Il s'agit de la première ligne de défense non seulement contre le malvertising et les malwares, mais aussi contre de nombreuses autres cybermenaces. Ces antivirus sont disponibles sur leurs sites officiels en version adaptée à chaque type d'appareil (Android, Windows, etc.). Il est aussi important de veiller à la mise à jour régulière de ces antivirus à partir de leurs sources officielles.

Renforcez la sécurité de vos appareils

3. Lancer des scans réguliers et complets sur vos appareils :

Lors de l'installation de l'antivirus sur votre appareil, il est important d'effectuer des analyses complètes de tous les fichiers et applications installés. Ces analyses sont facilement accessibles à travers leurs interfaces principales, ce qui permet de vous protéger contre tout type d'attaques ciblant vos appareils, notamment celles exploitant les publicités malveillantes et supprimer les malwares téléchargés à partir de ces dernières ou via d'autres sources.

4. Mettre à jour les différents logiciels et applications utilisés :

De nombreuses attaques de malvertising exploitent des failles de sécurité existantes sur vos appareils. Les mises à jour logicielles comprennent des correctifs de sécurité permettant de corriger ces failles. L'un des meilleurs moyens d'éviter ces attaques est donc de mettre à jour vos logiciels et applications à partir de leurs sources officielles. Il est important aussi de mettre à jour les systèmes d'exploitation de vos appareils (Windows, Android, etc.), à travers l'installation des derniers correctifs de sécurité que vous pouvez trouver sur les sites officiels ou bien directement à travers la fonctionnalité dédiée «mise à jour» qui se trouve par défaut dans la section «paramètres» de votre système.

Renforcez la sécurité de vos appareils

5.Être prudent lors de l'utilisation d'une connexion Wi-Fi gratuite de source inconnue :

Les connexions Wi-Fi gratuites de source inconnue, disponibles dans les espaces publics, ne sont pas sécurisées. En effet, un attaquant peut effectuer une connexion entre votre appareil et la source de connexion Wi-Fi pour effectuer des attaques de type (Man In The Middle). L'attaquant peut par la suite accéder à chacune des informations que vous envoyez sur Internet : e-mails importants, données de carte bancaire...etc. De même, certains attaquants créent des connexions Wi-Fi gratuites et vous incitent à se connecter pour récupérer toutes les informations transmises. Ces connexions peuvent même vous rediriger vers de fausses pages Web qui vous apparaitront légitimes et vous cibler facilement par les publicités malveillantes.

6. Télécharger les applications et les logiciels à partir des sources officielles

Il est recommandé de télécharger les applications et les logiciels à partir des sites officiels, tels que AppStore et PlayStore pour les applications mobiles. Autrement dit, si vous téléchargez des programmes ou applications à partir des sources inconnues ou à partir des sites non officiels, vous exposez vos appareils à des menaces malveillantes.

Renforcez la sécurité de vos appareils

7. Vérifier que les autorisations demandées par l'application lors de son installation sont nécessaires :

Lors de l'installation d'une application sur votre appareil, celle-ci demande des autorisations d'accès spécifiques pour son fonctionnement (Stockage, appareil photo, contacts, etc.). Il est recommandé, lors d'une installation, de vérifier que ces autorisations sont bien raisonnables avant de les approuver. Par exemple une application de Calculatrice qui demande un accès à l'appareil photo ou au microphone de votre appareil peut être une application suspecte, il est donc impératif de lui restreindre ce genre d'accès, voire ne pas l'installer et de chercher une application alternative.

8. Ne jamais utiliser des supports USB inconnus :

Les supports USB sont largement utilisés par les cybercriminels pour la propagation des logiciels malveillants. Lorsque vous connectez une clé USB inconnue à votre appareil, cette dernière peut contenir des programmes malveillants qui peuvent infecter votre appareil voire même le système d'information de votre organisme.

Guide pour les utilisateurs

Publicités malveillantes: *comment se prémunir?*

Renforcez la sécurité de vos appareils

COMMENT SE PRÉMUNIR DES PUBLICITÉS MALVEILLANTES ?

Installer des applicatifs de blocage des publicités sur les appareils à protéger

Télécharger les applications et les logiciels à partir des sources légitimes

Installer un antivirus professionnel tout en veillant à sa mise à jour régulière

Ne jamais utiliser des supports USB inconnus

Lancer des scans réguliers et complets sur vos appareils

Vérifier que les autorisations demandées par l'application sont nécessaires

Avoir prudence lors de l'utilisation d'une connexion Wi-Fi gratuite de source inconnue

Mettre à jour les différents logiciels et applications utilisés

2

GUIDE

POUR LES RESPONSABLES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Guide pour les RSSI

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

1.Mettre en place un DNS protector (PDNS)

Les publicités peuvent collecter des informations auprès des utilisateurs ou contenir des applications malveillantes cachées à l'intérieur, même si elles ne sont pas malveillantes, les publicités peuvent nuire aux performances d'un système et réduire son efficacité. Pour remédier à cette problématique, Il est recommandé de mettre en place un serveur DNS protector (PDNS) au niveau de votre organisme afin d'atténuer les risques liées au malvertising et renforcer le niveau de sécurité de votre réseau.

Le DNS peut être ciblé par différents types d'attaques, les cyberattaquants envoient régulièrement des paquets spécialement conçus aux serveurs DNS, afin de découvrir des vulnérabilités supplémentaires ou d'exploiter celles qui existent déjà, c'est à ce moment qu'entre en jeu le PDNS qui a une capacité de catégoriser les noms de domaine en fonction des renseignements sur les menaces. Les services PDNS exploitent généralement des flux d'informations open source, commerciaux et gouvernementaux de domaines malveillants connus.

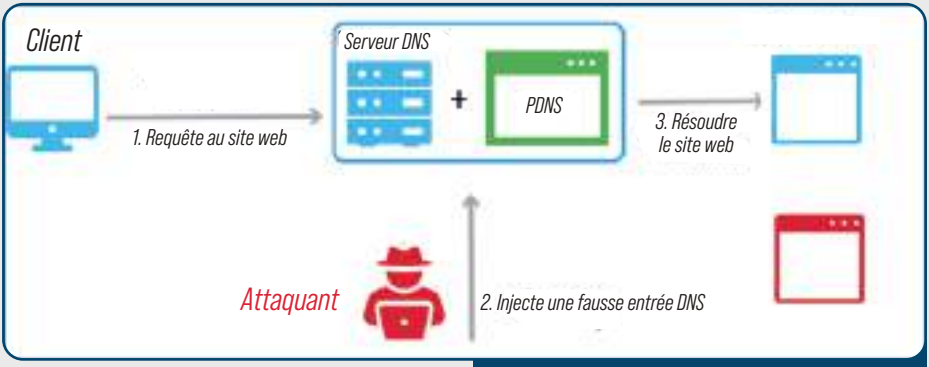


Figure: *empoisonnement DNS avec protection PDNS*

Les systèmes PDNS assurent une protection sur certaines cyberttaques telles que :

- *Publicités malveillantes ou indésirables.*
- *DNS Spoofing permettant le vol de données personnelles ;*
- *Phishing ;*
- *Malware et Ransomware ;*

Guide pour les RSSI

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

1.Mettre en place un DNS protector (PDNS)

POURQUOI DNS PROTECTOR ?

- ***Blocage des publicités :*** *bloquer les menaces liées au malvertising;*
- ***Protection contre des domaines de Phishing :*** *sites hébergeant des applications qui collectent des informations sur les utilisateurs ;*
- ***Protection contre des domaines contenant des distributions de logiciels malveillants :*** *sites connus pour diffusion des logiciels malveillants ;*
- ***Protection contre les sites Web offrant la possibilité de générer des domaines malveillants :*** *sites avec des noms de domaine générés par des logiciels malveillants*
- ***Vitesse améliorée :*** *les serveurs DNS sécurisés fournissent une recherche plus rapide que les serveurs DNS simples ;*
- ***Filtrage de contenu :*** *bloquer les sites dont le contenu appartient à des catégories classées interdites par rapport aux politiques d'accès d'une organisation.*
- ***Correction de faute de frappe :*** *pour corriger par exemple "organisme.dz" en "organism.dz ", les attaquants malveillants achètent souvent ces domaines "fautes de frappe" pour y installer des programmes malveillants ou en collecter des données ;*
- ***Un service PDNS*** *peut prendre plusieurs mesures (Action automatique prédéfinie) pour répondre à une requête de nom de domaine malveillante ou suspecte ;*
- ***Fournir*** *des alertes d'activité malveillante, des vues sur les indicateurs de l'organisme, une journalisation et une analyse historique, pour avoir une visibilité sur l'historique et en temps réel sur tout le trafic DNS sortant à des fins d'analyse et de réponse aux incidents.*

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

2.Isolation de la navigation

L'isolation de la navigation permet de séparer les processus de chargement des pages Web à partir des appareils utilisateur. Le code source des pages Web contenant une publicité malveillante ne s'exécute pas sur l'appareil de l'utilisateur, empêchant ainsi le risque d'infection.

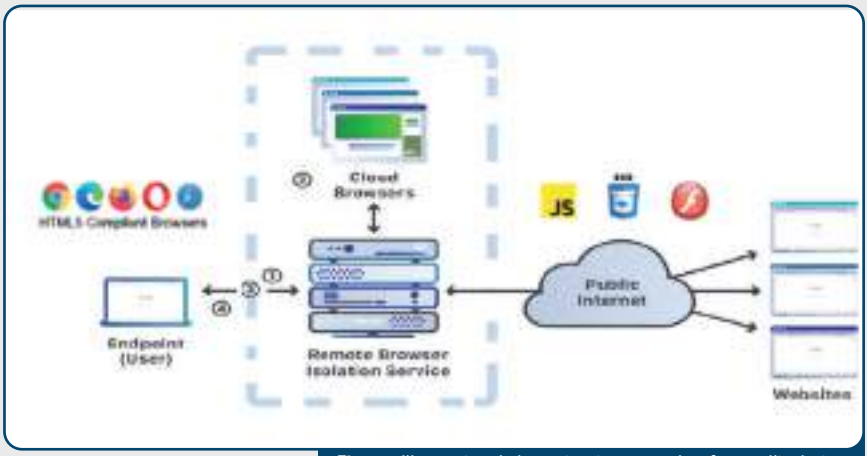


Figure: *Illustration de la navigation avec plateforme d'isolation*

AVANTAGES

- *Protège les utilisateurs des attaques ciblées masquées dans des pages Web, du contenu Web téléchargeable et des plug-ins vulnérables.*
- *Élimine la possibilité qu'une page Web n'exfiltre des données ou compromet l'appareil d'un utilisateur.*
- *Rend les attaques inconnues inoffensives.*

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

3.Gestion et surveillance des systèmes d'information

Dans le cadre de ses missions, le RSSI doit assurer l'activité de gestion et surveillance des systèmes d'information et veiller à la détection précoce des indices de compromission (indicateurs) liées aux publicités malveillantes afin de les contrecarrer.

Pour pouvoir mettre en place une solution de gestion de parc, il est nécessaire que cette dernière prenne en considération les éléments suivants :

- *La gestion d'inventaire des ressources informatiques ;*
- *La gestion du déploiement des systèmes d'exploitation (télé dépoilement) ;*
- *Le suivi et la traçabilité des équipements informatiques ;*
- *La garantie d'une visibilité totale sur les ressources (travaux de maintenance réalisés, Surveillance et dépannage des mises à jour logicielles et correctifs de sécurité ...etc.).*
- *Le suivi du cycle de vie des ressources informatiques pour un fonctionnement optimal.*

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

4. Configurer les pare-feux pour protéger le flux entrant

Un pare-feu de nouvelle génération (NGFW) est un système de sécurité informatique (matériel ou logiciel), qui a pour objectif d'examiner le trafic du réseau. Il reprend à son compte les fonctionnalités de filtrage de paquets, d'inspection du trafic, IPsec et des VPN. Il est capable de détecter et de bloquer les attaques sophistiquées en appliquant des règles de sécurité appropriées au niveau de toutes les couches du modèle TCP/IP, en particulier la couche applicative permettant le filtrage d'URL contenant des publicités malveillantes ainsi que le contrôle et la protection des utilisateurs et des applications contre les menaces cybernétiques.

POURQUOI UN FIREWALL ?

- *Identification et filtrage granulaire du trafic ;*
- *Séparation et démilitarisation des différents segments du réseau (niveau 7 - 5 ,4 ,2) ;*
- *Protection et détection d'intrusion IPS/IDS ainsi que la personnalisation des signatures, permettant de protéger les serveurs contre tous types d'intrusions ;*
- *Gestion de la Qualité de Service (QoS) pour limiter ou/et garantir une bande passante à un groupe d'utilisateurs ou à une application ;*
- *Analyse antivirale ;*
- *Fournir un VPN Site à Site et Client à Site (utilisateurs nomades) à partir de n'importe quel dispositif (PC portable, Tablette ou téléphone mobile) facilitant ainsi la mobilité des utilisateurs et administrateurs du Système d'Information ;*
- *Visibilité sur les utilisateurs contrôlés par l'Active Directory ;*

Guide pour les RSSI

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

5. Installer et configurer des antivirus au niveau des terminaux

Les publicités malveillantes endommagent les appareils de votre organisme, ainsi que les données qu'ils contiennent. Vos appareils peuvent être infectés en téléchargeant par inadvertance des logiciels malveillants qui se trouvent dans une pièce jointe liée à un e-mail frauduleux (spam), ou cachés sur une clé USB, ou même en visitant simplement un site Web douteux. Un antivirus et/ou un bloqueur de publicité malveillante installé et configuré d'une manière optimale au niveau de vos terminaux, contribuera sans doute à l'amélioration de la sécurité informatique de votre organisme.

Logiciels de sécurité endpoint

Les solutions de sécurité endpoint vous aident à défendre efficacement votre réseau et ses terminaux en centralisant leur administration, en authentifiant les connexions depuis tous les appareils et en assurant le déploiement et la mise à jour à distance des logiciels. Les solutions de sécurité endpoint rassemblent plusieurs applications de cyber-sécurité : antivirus, pare-feux, détecteurs d'intrusions, anti-malwares, etc.

VS

Logiciels antivirus

Les logiciels antivirus sont conçus pour détecter et supprimer les malwares, ils sont installés sur des appareils individuels comme les ordinateurs de bureau et les portables ou les téléphones mobiles, ainsi que sur des serveurs.

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

6. Limiter l'utilisation de Flash et JavaScript

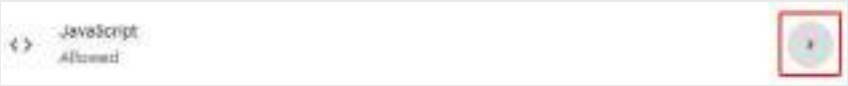
Un attaquant pourrait exploiter un site Web et collecter des données ou insérer un virus via les Codes JavaScript ou Flash injectés dans les panneaux publicitaires qui s'affichent sur les sites web y compris ceux qui sont réputés de confiance.

Exemple : Navigateur Chrome

1. *Dans le coin supérieur droit de la fenêtre Chrome, cliquez sur l' Icône du menu Chrome :* ⋮
2. *Sélectionnez **Paramètres** dans le menu déroulant*
3. *Sur le côté gauche de l'écran, cliquez sur **Confidentialité et sécurité***

4. *Développez l'option **Paramètres du site***

5. *Sur la page **Paramètres du site**, faites défiler jusqu'au bas de l'écran, sous la section **Contenu**, cliquez sur l'option **JavaScript** ;*



6. *À droite de l' option Autorisé , cliquez sur le bouton* *pour basculer entre les modes activer/désactiver JavaScript.*

*Pour autoriser ou bloquer JavaScript sur des sites Web spécifiques, dans la même fenêtre cliquez sur le bouton **Ajouter** dans la section bloquer ou autoriser pour ajouter des Liens de ces sites Web.*

Guide pour RSSI

Publicités malveillantes: *comment se prémunir?*

Pour les RSSI

*(**RSSI**: Responsable de la Sécurité des Systèmes d'Information)*

COMMENT SE PRÉMUNIR DES PUBLICITÉS MALVEILLANTES ?

Bloquer les sites compromis

Limiter l'utilisation de Flash et JavaScript

Isoler la navigation

Interdir l'installation de logiciels ne disposant pas de licences officielles.

Mettre en place DNS Protector

Installer et configurer des antivirus et AdBlockers au niveau des terminaux

Gérer et surveiller les systèmes d'information

Configurer les pare-feux pour protéger le flux entrant

3

GUIDE

POUR LES DÉVELOPPEURS

Pour les développeurs

1.Choisir soigneusement les AdNetworks

Les réseaux publicitaires ou AdNetworks sont un ensemble de serveurs dédiés tout comme les serveurs web, qui mettent en relation les annonceurs (Advertiser), du côté de la demande, et les éditeurs (Media/Developer), du côté de l'offre, afin de mener des campagnes publicitaires et maximiser les revenus des publicités. Pour faire face au phénomène des publicités malveillantes, le développeur doit opter pour le choix des « AdNetworks » les mieux réputés, non blacklistés et ne présentant aucun contenu malveillant tel que Google AdSense.

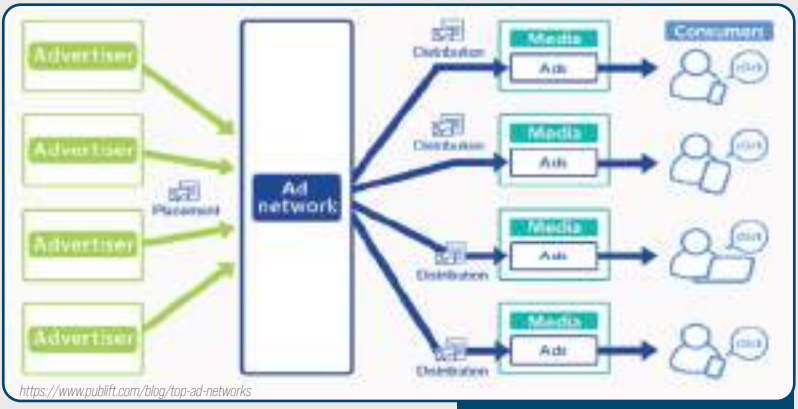


Figure: *Structure du réseau publicitaire*

Exemples d'AdNetworks réputés

Google AdSense
amazon ads
BuySellAds
media.net

Pour les développeurs

2.Elaborer une politique de sécurité du contenu
(Content Security Policy)

Une politique de sécurité de contenu (CSP) est une couche supplémentaire de protection du site Web, facile à mettre en œuvre et à contrôler. Le développeur ou l'éditeur du site peut utiliser une CSP pour détecter et atténuer les attaques de type Cross-Site Scripting (XSS) et d'injection de données.

Configurer une CSP permet au développeur de spécifier quel contenu est autorisé à être chargé. De cette façon, le développeur peut empêcher le téléchargement et l'exécution de scripts venant d'autres sources externes, le fonctionnement d'une CSP est décrit comme suit :

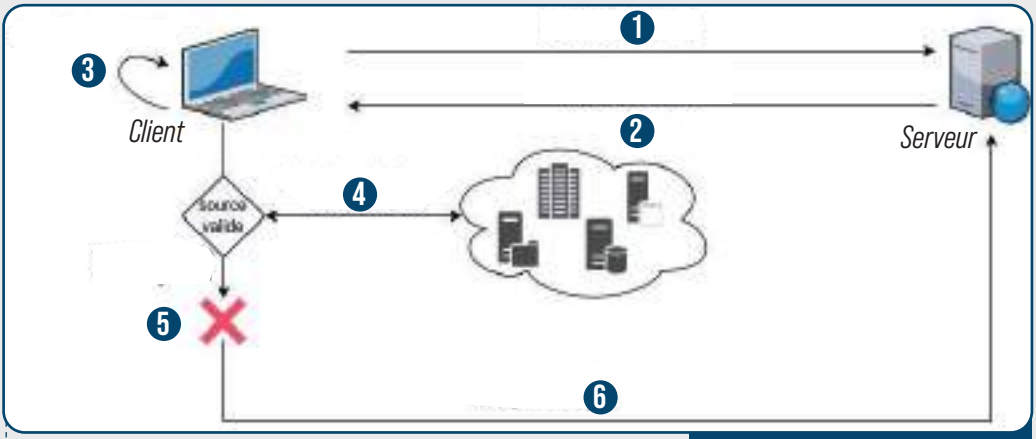


Figure: *Fonctionnement de la CSP*

1. *Un utilisateur visite le site web.*
2. *Le navigateur récupère les en-têtes du site Web.*
3. *Le navigateur analyse la CSP et enregistre les sources qui peuvent être chargées.*
4. *Le navigateur charge les ressources supplémentaires définies dans le code source du site web, comme Google Analytics, les polices, les images, les CSS, les scripts en ligne, etc.*
5. *Chaque source fait l'objet d'une référence croisée avec la CSP de la page, et si une source n'est pas spécifiée, la source est bloquée.*
6. *Si cette option est activée, un rapport de violation est envoyé du navigateur à un point de terminaison de rapport comme URIports.*

Pour les développeurs

3.Utiliser un Pare-feu d'application Web (WAF)

Le WAF (Web Application Firewall) ou le Pare-feu d'Applications Web est une solution de protection des applications web, qui filtre et surveille le trafic entre l'application Web et le réseau Internet. Il protège généralement les applications Web de plusieurs attaques notamment : Cross-Site Scripting (XSS) et SQL injection. Le WAF est également un type de proxy inversé qui protège le serveur web, en imposant le passage de tous les clients par ce proxy, avant d'atteindre le serveur web.

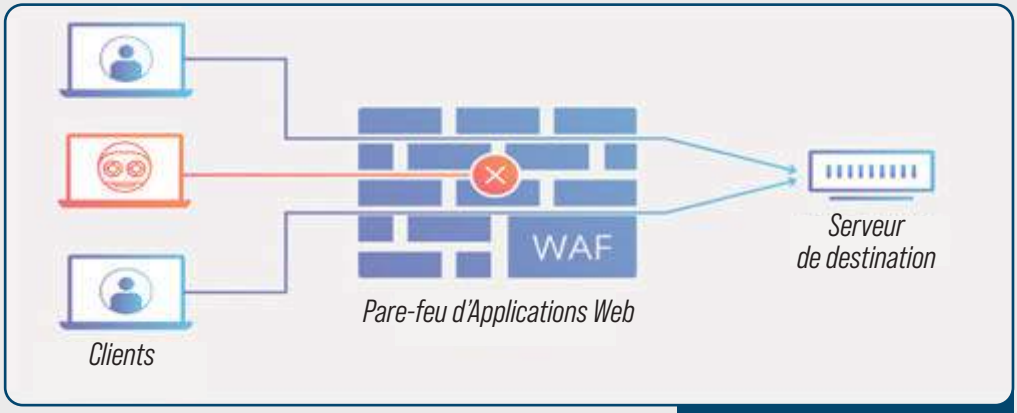
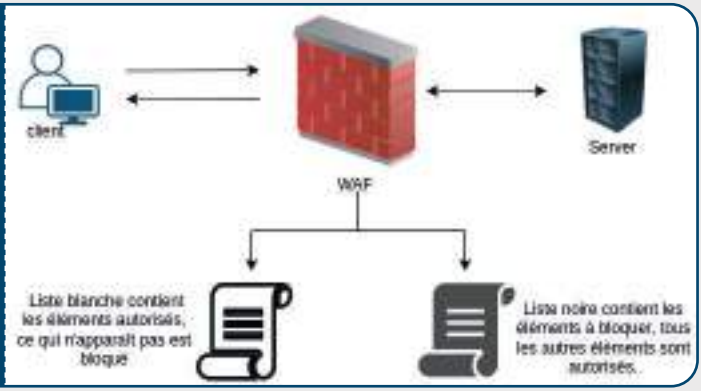


Figure: *Le Pare-feu d'Applications Web*

Les modèles de sécurité des WAF



Publicités malveillantes: *comment se prémunir?*

Pour les développeurs

4.Optez toujours pour HTML5 plutôt que Flash

La bibliothèque Flash comporte plusieurs failles de sécurité et de vulnérabilités. l'utilisation de cette bibliothèque est devenue déconseillée vu son obsolescence.

VULNÉRABILITÉS FLASH

- *le code exécutable ;*
- *le déni de service (DoS);*
- *le débordement (Buffer Overflow);*
- *les scripts intersites (XSS).*

Ces vulnérabilités sont exploitées par les cyberattaquants en injectant du code malveillant à travers les publicités qui font appel à la technologie Flash, ce qui a conduit de nombreux experts en sécurité à déconseiller son installation et à suggérer aux internautes d'utiliser des outils pour bloquer tout espace utilisant cette bibliothèque au niveau des pages Web.
Il existe maintenant de meilleures solutions dédiées pour l'animation à savoir HTML5 Canevas. Ce dernier est supporté par tous les navigateurs, plus performant et fonctionne sur tous les appareils. Vous n'avez pas besoin d'avoir un logiciel spécifique pour l'exécuter et présente moins de problèmes de sécurité concernant les publicités malveillantes.

AVANTAGES HTML5

- *PLUS DE SÉCURITÉ*
- *SIMPLICITÉ*
- *INTEROPÉRABILITÉ*
- *COMPATIBILITÉ*

Guide pour les développeurs

Publicités malveillantes: *comment se prémunir?*

Pour les développeurs

COMMENT SE PRÉMUNIR DES PUBLICITÉS MALVEILLANTES?

Choisissez soigneusement les AdNetworks

Utilisez un Web App Firewall

Optez toujours pour HTML5 plutôt que Flash

Elaborez une politique de sécurité du contenu

Crédit photos & ressources : www.freepik.com