Les PUP ou Programmes Potentiellement Indésirables

Pr Chérif DIALLO, CISSP
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" Le sage rejette toute influence indésirable et demeure centré." Lao Tseu, Philosophe.

Résumé: Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un fléau qui est très couramment rencontré dans l'utilisation d'un ordinateur, notamment lorsqu'il est souvent utilisé pour télécharger des logiciels sur le NET. Il s'agit des PUP qui sont des applications ou des programmes potentiellement indésirables qui se retrouvent sur l'ordinateur après avoir été intégrés dans d'autres logiciels qu'on a téléchargés. Leur identification peut s'avérer difficile, car ils sont souvent cachés. Cependant, il est important de comprendre comment ils se dissimulent. Un logiciel de nettoyage de logiciels peut également aider à détecter et supprimer les PUP, facilitant ainsi la tâche pour s'assurer que l'appareil demeure propre. Après la définition, nous donnerons quelques exemples et types de PUP, avant d'énumérer les solutions possibles et de conclure.

Mots clés: Cybersécurité, PUP, Adware, Spyware.

---

1. Définition

Les PUP (Potentially Unwanted Programs) ou les PPI (Programmes Potentiellement Indésirables) sont des logiciels potentiellement indésirables, qui sont intégrés à des packages de téléchargement et qui n'offrent aucun avantage aux utilisateurs. Les PUP sont généralement considérés comme des programmes indésirables, car ils n'offrent pas ou peu d'avantages et peuvent servir d'Adware (logiciel publicitaire) ou de Spyware (logiciel espion). Ils sont parfois également appelés applications potentiellement indésirables, et peuvent souvent compromettre la confidentialité et affaiblir la sécurité de votre ordinateur.

Les logiciels potentiellement indésirables regroupent :

- les logiciels qui affichent de la publicité intrusive dans Windows ou qui injectent des publicités dans les pages web que vous visitez (adwares ou logiciels publicitaires) ;
- les logiciels qui collectent vos informations personnelles (spywares ou logiciels espions) ;
- les logiciels qui ajoutent des barres d'outils dans votre navigateur web ;
- les logiciels qui ralentissent votre PC en raison de nombreux processus en arrière-plan.

Pour qualifier ces logiciels, il y a plusieurs définitions : PUP (Potentially Unwanted Programs), PUA (Potentially Unwanted Applications), LPI (Logiciels Potentiellement Indésirables) ou PPI (Programmes Potentiellement Indésirables).

2. Exemples de PUP

Savepath Deals, Superfish, V Play, JollyWallet, PDFProof, Clickware et Easy Speedtest sont quelques exemples courants de PUP. Les éditeurs qui conçoivent des programmes open source gratuits n'ont généralement pas les moyens de s'engager dans des batailles juridiques ou de contacter chaque site de téléchargement pour leur demander de dissocier leurs logiciels, ce qui explique que leurs applications sont souvent visées par les auteurs de PUP. Le lecteur multimédia VLC de VideoLAN est une cible fréquente du regroupement de PUP compte tenu de sa popularité. Beaucoup de logiciels PUP (mais pas tous) ciblent et exploitent l'utilisateur. Les conséquences d'un PUP sont très nombreuses. Ainsi, après avoir été téléchargé et installé sur votre ordinateur, un PUP peut malheureusement :

- Modifier la page d'accueil de votre navigateur.
- Ralentir votre ordinateur. Afficher des publicités envahissantes.
- Altérer les résultats des recherches. Ouvrir des fenêtres pop-up et pop-under.
- Voler vos informations privées. Suivre votre activité en ligne.

- Rajouter de nouvelles barres d'outils ou zones de recherche dans votre navigateur.
- Détourner votre navigateur. Faire apparaître de nouveaux favoris que vous n'aviez pas ajoutés.

Bien que ces activités soient embarrassantes, les PUP sont toujours considérés comme des « programmes potentiellement indésirables », car les utilisateurs ont formellement consenti à les télécharger. Ce consentement permet de mettre en doute le caractère illégal et indésirable des PUP et dissuade souvent les experts et spécialistes de Cybersécurité de les définir comme des malwares.

3. Types de PUP

Les principaux types de PUP sont :

- ***Adware (Logiciels publicitaires).*** Le type de PUP le plus courant est le logiciel publicitaire, communément appelé Adware. Les barres d'outils, souvent appelées barres de boutons, en sont l'exemple le plus connu. La plupart des utilisateurs ont peut-être, à un moment donné, ajouté une barre d'outils à leur navigateur. D'une manière générale, cela se produit accidentellement car les barres d'outils sont rarement utilisées. Presque généralement, ils sont installés sur un PC avec d'autres programmes gratuits. Les logiciels publicitaires sont, à bien des égards, le type de PUP le moins nocif, car son objectif principal est de surcharger un ordinateur de publicités via des pop-ups ou des barres. La publicité est assez irritante. Si l'utilisateur final clique sur les publicités, les choses peuvent devenir plus risquées. Ces clics peuvent lancer des sites Web, ajouter plus de PUP ou vous inciter à acheter des articles qui n'arriveront jamais parce que la publicité était frauduleuse. Outre les barres d'outils, les programmes potentiellement indésirables peuvent sembler bénéfiques. La majorité d'entre eux sont des applications qui vérifient le système. Ils effectuent cela pour identifier les défauts mineurs du système et libèrent les fichiers temporaires pour suppression. Cependant, pour effectuer l'optimisation, l'utilisateur doit souvent passer d'abord à un package premium qui exige très souvent un paiement ou un abonnement payant.
- ***Spyware (Logiciels espions).*** Les logiciels espions fonctionnent secrètement pour collecter des données personnelles et saisir l'historique du navigateur de l'ordinateur. Les utilisateurs peuvent obtenir des informations sensibles sur une autre personne via un logiciel espion, qui transmet ensuite ces informations à une autre partie. Étant donné que les logiciels espions peuvent conduire à l'usurpation d'identité, à la fraude, à l'effacement de fraudes ou d'activités illégales et à un ralentissement des performances de l'ordinateur, cette action a souvent des effets négatifs sur l'utilisateur. Cependant, les logiciels espions ne sont pas nécessairement dangereux ou risqués. Certains ont simplement été employés pour la publicité. Les logiciels espions collectent et stockent les informations des utilisateurs pour les faire fonctionner. Ensuite, ces données peuvent être vendues et utilisées pour afficher des publicités pop-up ou même suivre l'activité de l'utilisateur. Les rootkits, les balises Web, les téléphones résidentiels et les keyloggers (i.e. les enregistreurs de touches tapées au clavier) sont quelques types de logiciels espions.
- ***Browser hijacker (Pirate de navigateur).*** Un pirate de navigateur est un logiciel malveillant qui modifie les paramètres, l'apparence et le comportement d'un navigateur à l'insu de l'utilisateur. Ce logiciel nuisible est généralement utilisé par les fraudeurs et les criminels en ligne pour mener des activités telles que l'augmentation du trafic sur le site Web et des revenus publicitaires tout en obtenant les informations personnelles de l'utilisateur. Le moteur de recherche par défaut d'un utilisateur pourrait être changé par un navigateur piraté en un moteur avec beaucoup de publicité. Un navigateur qui a été pris en charge peut également conduire la recherche d'un utilisateur vers des sites Web peu recommandables. Des emplacements plus dangereux, tels que des logiciels malveillants, des logiciels publicitaires et d'autres Browser hijacker, peuvent être atteints via ces redirections. La méthode la plus courante de piratage d'un navigateur consiste à remplacer la page d'accueil par défaut ou d'autres sites Web par la page du Browser hijacker. En conséquence, les utilisateurs sont dirigés de force vers des pages publicitaires, augmentant ainsi le trafic vers les sites Web des Browser hijacker et générant plus de revenus pour eux.

4. Solutions

Les PUP sont souvent proposés en option lors de l'installation de logiciels gratuits. C'est un système qui permet aux éditeurs de logiciel de se financer (via des partenariats avec d'autres éditeurs) tout en conservant la gratuité de leurs logiciels. Le premier problème, ce sont les méthodes agressives voire trompeuses employées par les éditeurs pour forcer l'installation de ces PUP. C'est dans leur intérêt : ils sont rémunérés en fonction du nombre d'installation des PUP sur les PC des utilisateurs. Le second problème, ce sont les PUP eux-mêmes. Comme nous l'avons vu, ce sont probablement des Adwares ou des Spywares qui volent vos informations personnelles et affaiblissent la sécurité de votre PC. Face à ce problème, il faut donc :

- ***Lire le contrat de licence utilisateur final (CLUF).*** Le CLUF peut inclure une clause sur les PUP.
- ***S'éloigner des sites Web suspects***. Ceci est similaire à l'installation directe à partir du producteur. Les fournisseurs directs de programmes et de logiciels s'efforcent généralement de simplifier le processus de téléchargement de l'utilisateur et de se débarrasser de tous les PUP indésirables. D'autres sites Web tiers, en revanche, ont généralement d'autres objectifs que les fichiers ou programmes rendus accessibles au

téléchargement. Dans la plupart des cas, ces objectifs ne sont pas requis par l'utilisateur et finissent par mettre en danger à la fois l'utilisateur et le système utilisé. De plus, ces "sites suspects" peuvent agir comme un terrain fertile pour d'autres PUP facilement disponibles. En visitant involontairement les sites, les utilisateurs courent le risque d'installer l'un de ces programmes malveillants sur leur ordinateur. De plus, les pirates peuvent utiliser les sites Web pour collecter des données utilisateur à d'autres fins frauduleuses. Par conséquent, il est conseillé aux utilisateurs d'éviter de visiter des sites Web suspects. Téléchargez des logiciels à partir de sites Web de confiance. Soyez prudent lorsque vous téléchargez des logiciels gratuits ou des programmes de sociétés inconnues.

- ***Reconnaître les modèles d'obscurité.*** Il s'agit d'interfaces utilisateur qui ont été délibérément configurées pour tromper les utilisateurs. Ils sont conçus pour inciter les utilisateurs à prendre des mesures qu'ils n'auraient pas choisies de leur plein gré. À titre d'exemple, considérons un mailing où il est difficile de localiser le lien de désabonnement ou un site Web où il est difficile de localiser les coordonnées des clients.
- ***Choisir l'installation personnalisée.*** Au lieu d'utiliser les paramètres d'installation standard ou par défaut lors de l'installation du logiciel, choisissez les paramètres personnalisés ou avancés, qui sont généralement à l'abri des programmes potentiellement indésirables.
- ***Adopter une attitude prudente.*** Lors de l'installation d'un logiciel, il faut prendre soin de bien lire ce qui est affiché à l'écran. Prenez votre temps au lieu de cliquer seulement sur les boutons « Suivant » par négligence et avec frénésie.
- ***Activer la protection contre les PUP.*** Les logiciels antivirus proposent désormais une protection contre les PUP. Par défaut, cette protection n'est pas activée, il faut l'activer manuellement dans les paramètres de l'antivirus.
- ***Scanner les fichiers suspects avec votre anti-virus.*** Pour activer la protection contre les PUP, suivez les instructions suivantes selon l'antivirus que vous possédez :
  - Sur Avast Antivirus : Paramètres > Protection > Agents principaux > Logiciels potentiellement indésirables > Corriger automatiquement (à sélectionner).
  - Sur Avira Antivirus : Paramètres > Généralité > Catégories de dangers > Application potentiellement indésirable (à cocher).
  - Sur AVG Antivirus : Paramètres > Protection basique > Détections > Logiciels potentiellement indésirables > Corriger automatiquement (à sélectionner).
  - Sur Kaspersky Security Cloud : Paramètres > Général > Supprimer les outils malveillants, les logiciels publicitaires, les numérateurs automatiques et les logiciels de compression de données suspectés (à cocher).
  - Sur Windows Defender Antivirus : entrez la commande suivante dans PowerShell en tant qu'administrateur : **PS > | Set-MpPreference -PUAProtection 1**
- ***Supprimer les PUP, adwares et spywares.*** Pour supprimer les adwares (logiciels publicitaires), les spywares (logiciels espions) et tous les PUP de votre ordinateur, il y a plusieurs logiciels disponibles dont AdwCleaner. Mais, il est également assez simple de le faire sous Windows. En effet, voici comment supprimer les PUP de Windows :
  - Cliquez sur le bouton Démarrer, puis sur l'icône Paramètres.
  - Choisissez Applications dans le menu des paramètres Windows.
  - La section Applications et fonctionnalités comporte une liste de toutes les applications installées sur votre ordinateur. Dans cette liste, recherchez les PUP.
  - Sélectionnez le PUP identifié et cliquez sur Désinstaller.
- ***Nettoyer ensuite votre navigateur web (Firefox, Chrome, Safari, etc.)*** qui est sûrement infecté par des réglages ou des extensions malveillantes. Pour ce faire, réinitialiser votre navigateur dans sa configuration par défaut (votre historique et vos favoris seront conservés).

5. Pour finir

N'hésitez pas à analyser périodiquement (environ une fois par mois) votre ordinateur afin de supprimer tous les Adwares et Spywares qui ont réussis à pénétrer dans votre PC. Vous pouvez également utiliser le scanner de votre logiciel antivirus. Il est bon de savoir rechercher manuellement des PUP sur son ordinateur, mais si vous ne savez pas trop comment procéder ou si vous n'êtes pas certain d'avoir trouvé tous les PUP, utilisez un outil logiciel qui effectue cette tâche automatiquement.

Enfin, il faut noter qu'en 2015, une étude a mentionné que la plupart des sites de téléchargement gratuit regroupaient leurs téléchargements avec des PUP (et que download.com était le pire). D'autres études ont montré avec consternation que « malheureusement, même sur le moteur de recherche Google, tous les meilleurs résultats pour la plupart des logiciels libres et open source ne sont que des annonces pour des sites qui regroupent des PUP avec les logiciels désirés ».