Publicité malveillante et cette cybermenace n’est pas sur le dark web, mais sur Google
Malwarebytes

David Ruiz ⋮

Sur Internet, les gens ne doivent pas se contenter d’ouvrir des pièces jointes suspectes ou de saisir leurs informations sensibles sur des sites Web nuisibles, ils doivent également se soucier de leurs recherches Google.

En effet, l’année dernière, comme l’a révélé notre rapport 2024 sur l’état des logiciels malveillants ThreatDown, les cybercriminels ont afflué vers une méthode de *diffusion* de logiciels malveillants qui ne nécessite pas qu’ils connaissent l’adresse courriel, les identifiants de connexion, les informations personnelles ou quoi que ce soit d’autre.

Au lieu de cela, les cybercriminels n’ont qu’à tromper quelqu’un pour qu’il clique sur un résultat de recherche qui semble remarquablement légitime.

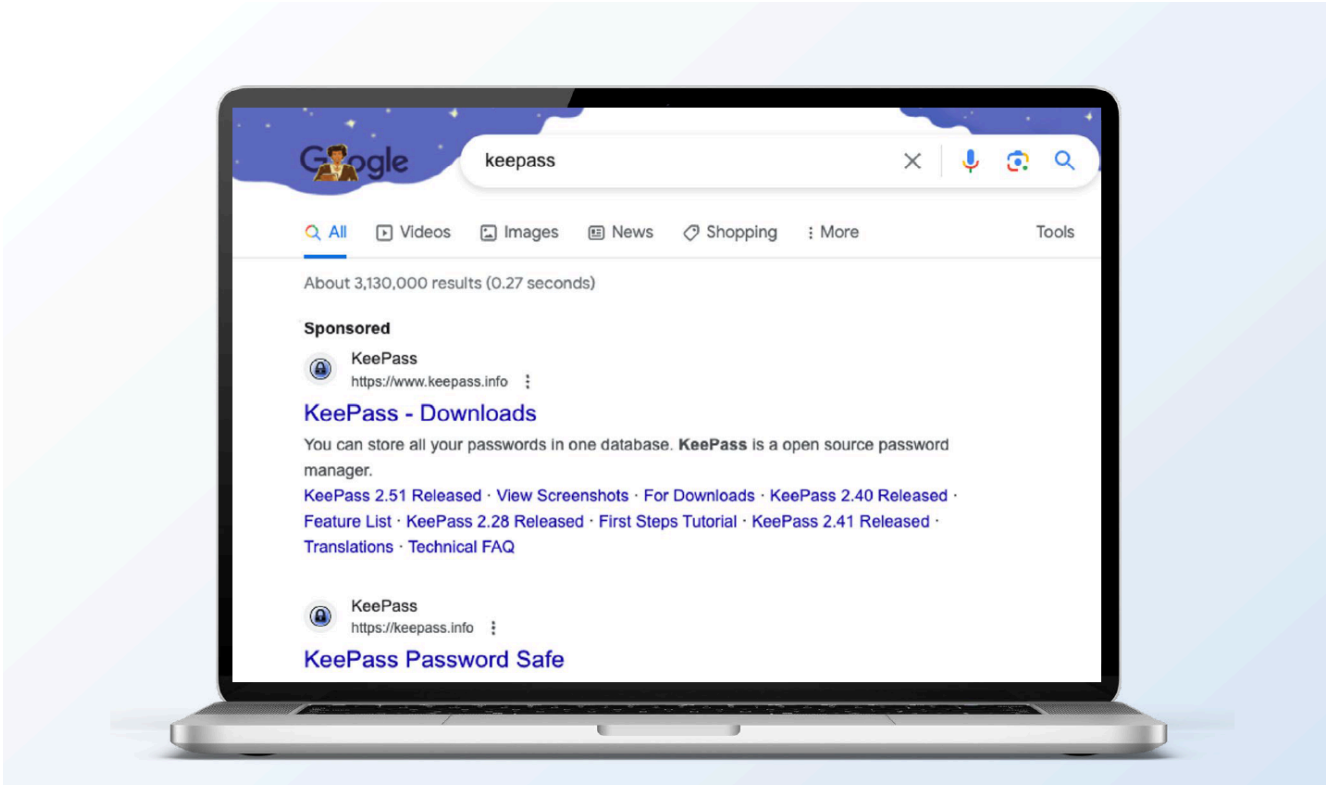
C’est le travail de la « publicité malveillante », ou « publicité malveillante », en abrégé.
La publicité malveillante n’est pas un logiciel malveillant en soi.

Au lieu de cela, il s'agit d'un processus sournois consistant à placer des logiciels malveillants, des virus ou d'autres cyberinfections sur l'ordinateur, la tablette ou le téléphone intelligent d'une personne.
Les logiciels malveillants qui finissent par se glisser sur l'appareil d'une personne se présentent sous de nombreuses formes, mais les cybercriminels ont tendance à privilégier les logiciels malveillants qui peuvent voler les identifiants et les informations de connexion d'une personne.
Avec ces informations nouvellement volées, les cybercriminels peuvent ensuite accéder à des comptes en ligne sensibles appartenant à la victime.

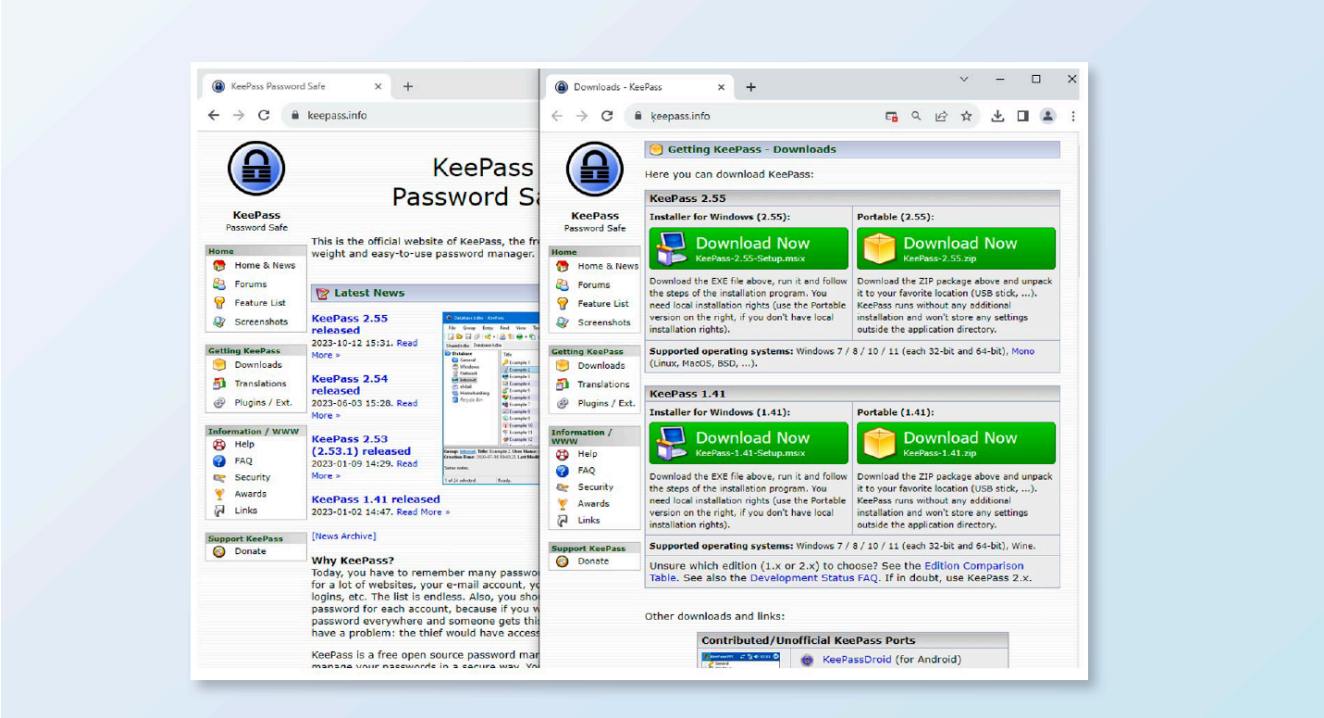
Mais avant que ce vol numérique ne puisse se produire, les cybercriminels doivent d'abord piéger une victime, et ils le font en abusant de l'infrastructure publicitaire numérique qui sous-tend les résultats de recherche Google.

Pensez à rechercher sur Google « chaussures de course » : vous verrez probablement des publicités pour Nike et Adidas.
Une recherche Google pour « meilleur bagage à main » produira invariablement des publicités pour les marques grand public Monos et Away.
Et une recherche Google pour une marque comme Amazon affichera, comme prévu, des publicités pour Amazon.

Mais les cybercriminels le savent, et en réponse, ils ont créé des publicités qui *semblent* légitimes, mais dirigent plutôt les victimes vers des sites Web malveillants qui contiennent des logiciels malveillants.
Les sites Web eux-mêmes, eux aussi, présentent une ressemblance frappante avec le produit ou la marque qu'ils imitent, afin de maintenir une mascarade de légitimité.
À partir de ces sites Web, les utilisateurs téléchargent ce qu'ils pensent être un logiciel valide, téléchargeant plutôt des logiciels malveillants qui les exposent à d'autres attaques.



Une publicité malveillante pour le gestionnaire de mots de passe KeePass apparaît comme une publicité légitime.



Le vrai site web de KeePass (à gauche) côte à côte avec un site de publicité malveillante (à droite).

Il est vrai que la publicité malveillante est souvent considérée comme un risque pour les entreprises, mais les sites Web imitateurs créés par les cybercriminels peuvent également usurper l'identité de marques populaires pour les utilisateurs quotidiens.

Comme l'a révélé notre rapport 2024 sur l'état des logiciels malveillants ThreatDown, les cinq marques les plus usurpées pour la publicité malveillante l'année dernière sont les suivantes :

1. Amazon
2. Rufus
3. Weebly (en anglais seulement)
4. NotePad++
5. TradingView (en anglais seulement)

Ces cinq marques n'ont peut-être pas toutes la même familiarité, mais leurs produits et services suscitent l'intérêt d'un large éventail d'utilisateurs, des produits de création de sites Web de Weebly à la plate-forme de trading d'investissement de TradingView, en passant par l'outil de démarrage de système d'exploitation portable de niche mais utile de Rufus.

Pourquoi l'augmentation des publicités malveillantes l'année dernière ?

Si les annonces Google existent depuis plus d'une décennie, pourquoi ne sont-elles utilisées que par les cybercriminels aujourd'hui ?

La vérité est que la publicité malveillante existe depuis des années, mais une résurgence particulière a été enregistrée plus récemment.

En 2022, les cybercriminels ont perdu l'accès à l'une de leurs méthodes préférées de diffusion de logiciels malveillants.

Cet été-là, Microsoft a annoncé qu'il bloquerait enfin les « macros » intégrées dans des fichiers téléchargés sur Internet.
Les macros sont essentiellement des instructions que les utilisateurs peuvent programmer afin que plusieurs tâches puissent être regroupées.
Le danger, cependant, est que les cybercriminels préprogramment des macros dans certains fichiers pour Microsoft Word, Excel ou PowerPoint, puis envoient ces fichiers sous forme de pièces jointes malveillantes.
Une fois ces pièces jointes téléchargées et ouvertes par les utilisateurs, les macros intégrées déclenchaient un ensemble d'instructions ordonnant à l'ordinateur d'une personne d'installer un logiciel malveillant à partir d'un site Web dangereux en ligne.

Les macros ont été un fléau pour la cybersécurité pendant des années, car elles étaient efficaces et faciles à mettre en œuvre.

Mais lorsque Microsoft a restreint les capacités de macro en 2022, les cybercriminels ont dû trouver un autre canal de diffusion de logiciels malveillants.
Ils se sont concentrés sur la publicité malveillante.

La publicité malveillante d'aujourd'hui est de plus en plus sophistiquée, car les cybercriminels peuvent créer et acheter des publicités en ligne qui ciblent des types spécifiques d'utilisateurs en fonction de l'emplacement et des données démographiques. Il est inquiétant de constater que la publicité malveillante moderne peut même éviter la détection de fraude de base, car les cybercriminels peuvent créer des sites Web qui déterminent si un utilisateur est une personne réelle ou simplement un robot qui parcourt le Web pour trouver et signaler une activité malveillante.

Comment se protéger contre les publicités malveillantes

La menace de la publicité malveillante est multidimensionnelle : il y a les publicités frauduleuses que les cybercriminels placent sur les résultats de recherche Google, les sites Web malveillants qui imitent des marques et des entreprises légitimes pour convaincre les utilisateurs de télécharger des logiciels malveillants, et l'infection par des logiciels malveillants elle-même.

En tant que telle, toute stratégie de défense réussie doit être à plusieurs niveaux.

Pour naviguer en toute sécurité, les gens peuvent compter sur Malwarebytes Browser Guard, une extension de navigateur qui bloque le suivi des tiers et signale les sites Web malveillants connus pour être sous le contrôle des cybercriminels.
Comme nous l'avons écrit précédemment :

> « Malwarebytes Browser Guard offre une protection supplémentaire aux fonctionnalités standard de blocage des publicités en couvrant une plus grande zone de la chaîne d'attaque jusqu'aux

domaines contrôlés par les attaquants.
Grâce à son moteur heuristique intégré, il peut également bloquer de manière proactive les sites Web malveillants jamais vus auparavant.

Le problème avec la publicité malveillante, cependant, est que de nouveaux sites Web malveillants sont créés chaque jour.
Les défenseurs de la cybersécurité sont donc souvent pris dans un jeu de rattrapage.

Ici, les utilisateurs peuvent trouver la sécurité de Malwarebytes Premium, qui fournit une protection en temps réel pour détecter et arrêter toutes les cybermenaces qui s'installent sur un appareil, même si ces menaces se font passer pour des applications ou des logiciels légitimes.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240226
"C'est ensemble qu'on avance"