krebsonsecurity.com /2024/01/using-google-search-to-find-software-can-be-risky/

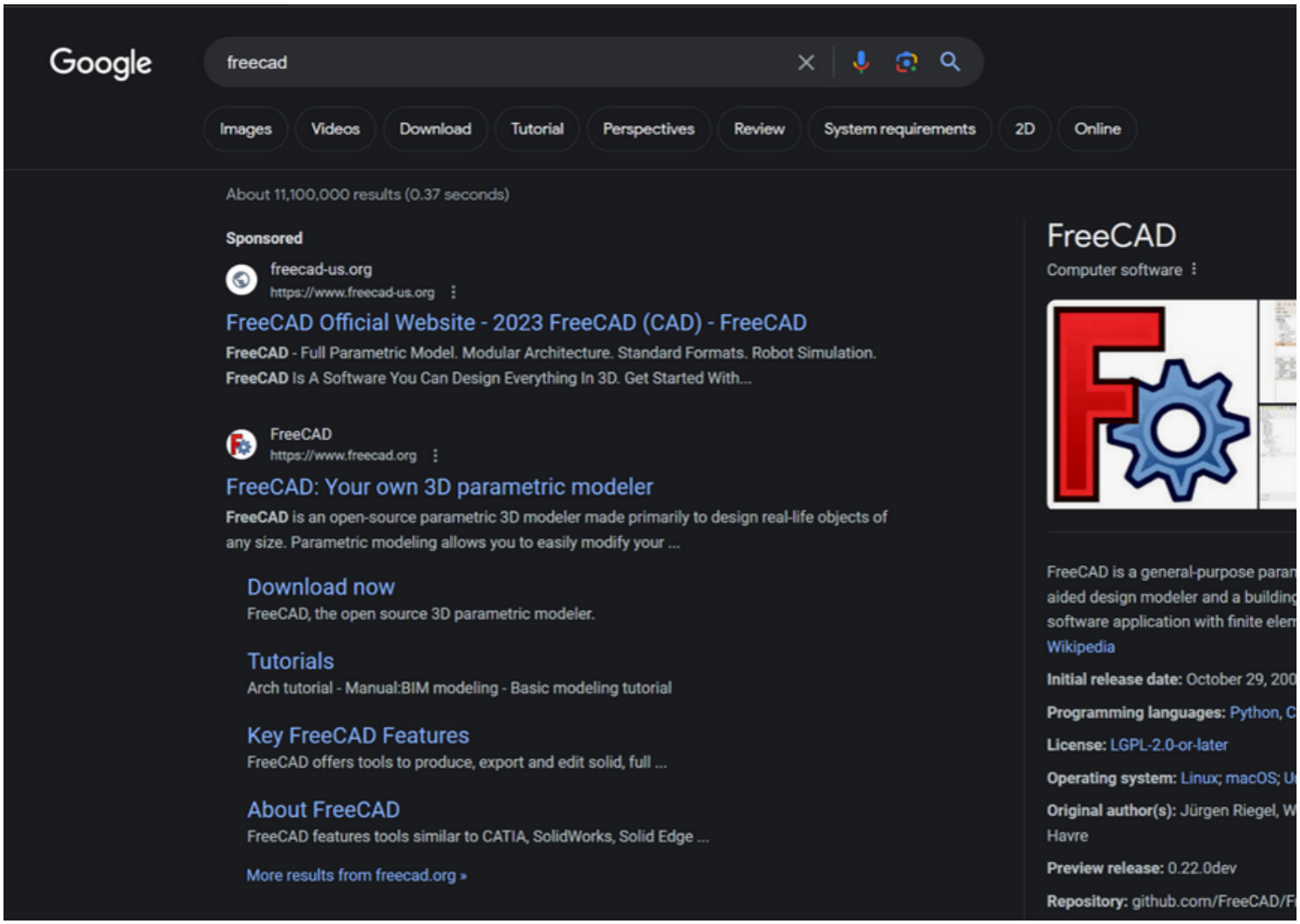
Utiliser la recherche Google pour trouver un logiciel peut être risqué

Google continue de lutter contre les cybercriminels qui diffusent des publicités malveillantes sur sa plate-forme de recherche pour inciter les gens à télécharger des copies piégées d'applications logicielles gratuites populaires.
Les publicités malveillantes, qui apparaissent au-dessus des résultats de recherche naturels et précèdent souvent les liens vers des sources légitimes du même logiciel, peuvent rendre la recherche de logiciels sur Google une affaire risquée.

Google affirme qu'assurer la sécurité des utilisateurs est une priorité absolue et que l'entreprise dispose d'une équipe de plusieurs milliers de personnes travaillant 24 heures sur 24 pour créer et appliquer ses politiques en matière d'abus.
Et selon la plupart des témoignages, la menace des mauvaises publicités menant à des logiciels détournés a considérablement diminué par rapport à il y a un an .

Mais les cybercriminels trouvent constamment des moyens ingénieux de passer sous le radar anti-abus de Google, et de nouveaux exemples de mauvaises publicités menant à des logiciels malveillants sont encore trop courants.

Par exemple, une recherche Google plus tôt cette semaine pour le programme de conception graphique gratuit **FreeCAD** a produit le résultat suivant, qui montre qu'une annonce « sponsorisée » en haut des résultats de recherche fait la publicité du logiciel disponible sur freecad-us[.]org.
Bien que ce site Web prétende être le site Web officiel de FreeCAD, cet honneur appartient au résultat situé directement en dessous : le site légitime freecad.org.



Comment savons-nous que freecad-us[.]org est malveillant ?
Un examen sur **DomainTools.com** montre que ce domaine est le plus récent (enregistré le 19 janvier 2024) de plus de 200 domaines à l'adresse Internet **93.190.143[.]252** qui ressemblent à des titres de logiciels populaires, y compris **Dashlane-project[. .]com** , **filezillasoft[.]com** , **keepermanager[.]com** et **libreofficeproject[.]com** .

Certains des domaines de cet hébergeur néerlandais semblent n'être rien de plus que des sites Web d'évaluation de logiciels qui volent le contenu de sources d'informations établies dans le monde informatique, notamment **Gartner** , **PCWorld** , **Slashdot** et **TechRadar** .

D'autres domaines à l'adresse 93.190.143[.]252 servent effectivement à télécharger des logiciels, mais aucun d'entre eux n'est susceptible d'être malveillant si l'on visite les sites via une navigation directe.
Si l'on visite **openai-project[.]org** et télécharge une copie de l'application de gestion de bureau Windows populaire **Rainmeter** , par exemple, le fichier téléchargé a la même signature de fichier exacte que le véritable programme d'installation de Rainmeter disponible sur rainmeter.com.

Mais ce n'est qu'une ruse, estime **Tom Hegel** , chercheur principal en menaces au sein de la société de sécurité **Sentinel One** .
Hegel suit ces domaines malveillants depuis plus d'un an, et il a déclaré que les sites de téléchargement de logiciels apparemment inoffensifs deviendront périodiquement malveillants, remplaçant les copies légitimes de

logiciels populaires par des versions dérobées qui permettront aux cybercriminels de contrôler les systèmes à distance.

"Ils utilisent l'automatisation pour extraire du faux contenu, et ils hébergent et renoncent à des logiciels malveillants", a déclaré Hegel, soulignant que les téléchargements malveillants ne peuvent être proposés qu'aux visiteurs provenant de zones géographiques spécifiques, comme les États-Unis.
"Dans les campagnes publicitaires malveillantes que nous avons vues liées à ce groupe, ils attendaient que les domaines gagnent en légitimité sur les moteurs de recherche, puis tournaient la page pendant environ un jour, puis revenaient en arrière."

En février 2023, Hegel a co-écrit un rapport sur ce même réseau, que Sentinel One a baptisé **MalVirt** (une pièce de théâtre sur la « publicité malveillante »).
Ils ont conclu que l'augmentation des publicités malveillantes usurpant divers produits logiciels était directement responsable de l'augmentation des infections par des chevaux de Troie infostealer comme **IcedID** , **Redline Stealer** , **Formbook** et **AuroraStealer** .

Hegel a noté que l'augmentation des publicités sur le thème des logiciels malveillants est survenue peu de temps après que Microsoft a commencé à bloquer par défaut les macros Office dans les documents téléchargés sur Internet.
Il a déclaré que le volume des campagnes publicitaires malveillantes actuelles de ce groupe semble être relativement faible par rapport à il y a un an.

« Il semble que la même campagne se poursuive », a déclaré Hegel.
« En janvier dernier, chaque recherche Google sur « Autocad » aboutissait à quelque chose de mauvais.
Maintenant, c'est comme s'ils payaient Google pour obtenir une recherche sur une douzaine.
Je suppose que cela continue en raison des hauts et des bas des domaines hébergeant des logiciels malveillants et qui semblent légitimes.

Plusieurs sites Web de cet hôte néerlandais (93.190.143[.]252) sont actuellement bloqués par la technologie Safebrowsing de Google et étiquetés avec un avertissement rouge bien visible indiquant que le site Web tentera d'imposer des logiciels malveillants aux visiteurs qui ignorent l'avertissement et continuent.

Mais la raison pour laquelle Google n'a pas bloqué davantage de 240+ autres domaines chez ce même hôte, ou bien ne les a pas entièrement supprimés de son index de recherche, reste un mystère.
D'autant plus qu'il n'y a rien d'autre que ces domaines hébergés à cette adresse IP néerlandaise et qu'ils sont tous restés à cette adresse au cours de l'année écoulée.

En réponse aux questions de KrebsOnSecurity, Google a déclaré que le maintien d'un écosystème publicitaire sécurisé et la suppression des logiciels malveillants sur ses plates-formes étaient une priorité pour Google.

"Les acteurs malveillants emploient souvent des mesures sophistiquées pour dissimuler leur identité et échapper à nos politiques et à leurs applications, montrant parfois une chose à Google et une autre aux utilisateurs", a déclaré Google dans une déclaration écrite.
« Nous avons examiné les annonces en question, supprimé celles qui enfreignaient nos politiques et suspendu les comptes associés.
Nous continuerons à surveiller et à appliquer nos protections.

Google affirme avoir supprimé 5,2 milliards de publicités en 2022, restreint plus de 4,3 milliards de publicités et suspendu plus de 6,7 millions de comptes d'annonceurs.
Le dernier rapport de la société sur la sécurité des publicités indique que Google a bloqué ou supprimé en 2022 1,36 milliard de publicités pour violation de ses politiques en matière d'abus.

Certains des domaines référencés dans cette histoire ont été inclus dans le rapport de Sentinel One de février 2023, mais des dizaines d'autres ont été ajoutés depuis, comme ceux usurpant les sites de téléchargement officiels de **Corel Draw** , **Github Desktop** , **Roboform** et **Teamviewer** .

Ce rapport d'octobre 2023 sur le forum des utilisateurs de FreeCAD provient d'un utilisateur qui a déclaré avoir téléchargé une copie du logiciel depuis freecadsoft[.]com après avoir vu le site promu en haut d'un résultat de recherche Google pour « freecad ». Près d'un mois plus tard, un autre utilisateur de FreeCAD a déclaré avoir été piqué par la même arnaque.

« Cela m'a eu », a écrit « Matterform » un utilisateur du forum FreeCAD le 19 novembre 2023.
« Veuillez laisser un rapport à Google afin qu'il puisse le signaler.
Ils ont payé Google pour des publications sponsorisées.

Le rapport de Sentinel One n'a pas approfondi le « qui » derrière cette campagne MalVirt en cours, et il existe peu d'indices précieux qui pointent vers une attribution.
Tous les domaines en question ont été enregistrés via **webnic.cc** , et plusieurs d'entre eux affichent une page d'espace réservé indiquant que le site est prêt à accueillir du contenu.
L'affichage de la source HTML de ces pages d'espace réservé montre que la plupart des commentaires cachés dans le code sont en cyrillique.

Essayer de suivre les escrocs à l'aide des outils Ad Transparency de Google n'a pas mené loin.
L'enregistrement de transparence de l'annonce malveillante mettant en vedette freecad-us[.]org (dans la capture d'écran ci-dessus) montre que le compte publicitaire utilisé pour payer l'annonce n'a diffusé qu'une seule annonce via la recherche Google : il faisait la publicité d'un site Web de photographie de mariage dans Nouvelle-Zélande.

Le propriétaire apparent de ce site Web de photographie n'a pas répondu aux demandes de commentaires, mais il est également probable que son compte publicitaire Google ait été piraté et utilisé pour diffuser ces publicités malveillantes.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
2024125
"C'est ensemble qu'on avance"