Les applications Google vecteurs de malwares.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 22/11/2023 13:00:00

Le Threat Labs de Netskope dÃ©voile sa nouvelle Ã©tude appelant les professionnels du secteur du retail Ã la vigilance : contrairement Ã dâ□□autres secteurs oÃ¹ Microsoft OneDrive est Ã la fois lâ□□application la plus utilisÃ©e et la plus prisÃ©e pour tÃ©lÃ©charger des logiciels malveillants, les applications Google constituent le principal vecteur de diffusion de logiciels malveillants dans le retail.

Si OneDrive est lâ□□application la plus utilisÃ©e par les professionnels de ce secteur, Google Drive et Google Gmail occupent les deux premiÃ¨res places pour la diffusion de malwares dans ce secteur. Les chevaux de Troie constituent le principal mÃ©canisme dâ□□attaque, incitant les utilisateurs Ã tÃ©lÃ©charger dâ□□autres logiciels malveillants.

De nombreuses familles de malwares ont pour mission de subtiliser des informations bancaires, des identifiants de connexion, des donnÃ©es personnelles, ainsi que des informations liÃ©es aux cartes bancaires.

La popularitÃ© de WhatsApp est Ã©galement bien supÃ©rieure Ã celle des autres secteurs - en moyenne, cette application y est en effet trois fois plus utilisÃ©e que dans les autres secteurs verticaux, se classant seulement aprÃ¨s OneDrive en termes de nombre de tÃ©lÃ©chargements et de tÃ©lÃ©versements.

Or, cette situation soulÃ¨ve un risque majeur, non seulement parce que WhatsApp est un canal couramment exploitÃ© pour diffuser des contenus malveillants, tels que les malwares et pages de phishing, mais Ã©galement parce que ces chiffres laissent entendre que le secteur du retail plÃ©biscite lâ□□utilisation dâ□□une application de messagerie instantanÃ©e personnelle en tant quâ□□outil de collaboration dâ□□entreprise, ce qui accroÃ®t le risque de vol ou dâ□□exposition des donnÃ©es. A titre dâ□□exemple, il est trÃ¨s facile de transfÃ©rer un message Ã©changÃ© sur WhatsApp.

Â«â□□Les attaquants exploitent des applications cloud dans le but de passer inaperÃ§us et dâ□□Ã©chapper aux contrÃ´les de sÃ©curitÃ© traditionnels qui nâ□□inspectent pas le trafic dans le cloud, explique Ray Canzanese, Director of Netskope Threat Labs. A lâ□□approche des fÃªtes de fin dâ□□annÃ©e, les employÃ©s du retail et les consommateurs doivent redoubler de vigilance, car les activitÃ©s de phishing, les vols dâ□□identifiants et lâ□□utilisation de logiciels malveillants ont tendance Ã augmenter dans ce secteur pendant cette pÃ©riode.â□□Â»

Si la frÃ©quence de diffusion des logiciels malveillants dans le retail a, de maniÃ¨re gÃ©nÃ©rale, suivi le modÃ¨le des autres secteurs au cours des 12 derniers mois, les pÃ©riodes de pointe â□□ câ□□est-Ã -dire les mois dâ□□avril, mai et juin de cette annÃ©e â□□ se sont caractÃ©risÃ©es par le nombre comparativement Ã©levÃ© de malwares diffusÃ©s dans le secteur du retail via des applications cloud. En avril par exemple, 70 % des logiciels malveillants diffusÃ©s ont exploitÃ© des applications cloud, soit 10 % de plus que dans les autres secteurs dâ□□activitÃ©.

Le rapport rÃ©vÃ¨le en outre que Google Drive, Google Gmail et WhatsApp figurent dans le Top 5 des applications les plus utilisÃ©es pour les tÃ©lÃ©chargements dans le retail, toutes trois affichant une popularitÃ© nettement supÃ©rieure aux autres secteurs dâ□□activitÃ© :

â¢ Google Drive est utilisÃ© par 34 % des professionnels du retail contre 19 % dans les autres secteurs dâactivitÃ©.
â¢ Gmail est employÃ© par 21 % des utilisateurs de ce secteur contre 13 % dans les autres secteurs dâactivitÃ©.
â¢ WhatsApp est utilisÃ© par 17 % des utilisateurs du retail contre 5,9 % dans les autres domaines, ce qui en fait une application plus populaire que Sharepoint.

Le Threat Labs de Netskope recommande par consÃ©quent aux entreprises qui opÃ¨rent dans le secteur du retail de prendre les mesures suivantes pour corriger leur posture de sÃ©curitÃ© :

â¢ ProcÃ©der Ã une inspection approfondie des tÃ©lÃ©chargements HTTP et HTTPS afin dâÃ©viter lâinfiltration de logiciels malveillants.
â¢ Effectuer une analyse en profondeur des types de fichiers Ã haut risque en amont des tÃ©lÃ©chargements en utilisant des outils de protection contre les menaces avancÃ©es.

â¢ Appliquer des rÃ¨gles capables de bloquer le tÃ©lÃ©chargement et le tÃ©lÃ©versement dâapplications inutiles en vue de rÃ©duire la surface dâexposition aux risques.
â¢ Mettre en Åuvre un systÃ¨me de prÃ©vention des intrusions (IPS) dans le but dâidentifier et de bloquer les schÃ©mas de trafic malveillants.
â¢ Adopter la technologie dâisolation de navigateur Ã distance (RBI) pour maximiser la protection lors de la visite dâun site Web.

Pour consulter cette Ã©tude dans son intÃ©gralitÃ©.