Des malwares dans des applications, la hausse vertigineuse.
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 11/1/2023 14:00:00

Netskope, leader sur le marchÃ© du SASE (Secure Access Service Edge), dÃ©voile une nouvelle Ã©tude selon laquelle plus de 400â□□applications cloud diffÃ©rentes ont diffusÃ© des logiciels malveillants en 2022, soit prÃ¨s de trois fois plus quâ□□en 2021.

Les chercheurs de Netskope ont Ã©galement constatÃ© que 30â□□% des tÃ©lÃ©chargements de malwares sur le cloud en 2022 provenaient de Microsoft OneDrive.

Les applications cloud sont abondamment utilisÃ©es par les entreprises ; cette situation nâ□□Ã©chappe pas aux attaquants, lesquels en font un outil de choix pour hÃ©berger des logiciels malveillants et causer des dommages.

Lâ□□Ã©tude, intitulÃ©e Â« Cloud & Threat Report Â» et publiÃ©e par le Threat Labs de Netskope, analyse la maniÃ¨re dont Ã©voluent ces tendances relatives Ã la sÃ©curitÃ© du cloud et apporte des conseils qui permettent aux entreprises dâ□□amÃ©liorer leur posture de sÃ©curitÃ© en fonction de ces changements.

Â«â□□Les cybercriminels exploitent de faÃ§on croissante les applications cloud critiques dans le but de diffuser des logiciels malveillants en contournant des contrÃ´les de sÃ©curitÃ© inadaptÃ©s, explique Ray Canzanese, Threat Research Director du Threat Labs de Netskope.

Il est par consÃ©quent impÃ©ratif que davantage dâ□□entreprises inspectent la totalitÃ© de leur trafic HTTP et HTTPS, notamment pour les applications cloud les plus couramment utilisÃ©es, quâ□□elles soient professionnelles ou personnelles, dans lâ□□optique dâ□□identifier des contenus malveillants.â□□Â»

L'augmentation des tÃ©lÃ©chargements vers les applications cloud entraÃ®ne une augmentation des tÃ©lÃ©chargements de malwares

Le changement le plus significatif concernant les applications cloud en 2022, par rapport Ã 2021, est l'augmentation marquÃ©e du pourcentage d'utilisateurs tÃ©lÃ©chargeant du contenu sur le cloud.

Selon lâ□□Ã©tude de Netskope en effet, plus de 25â□□% des utilisateurs du monde entier ont tÃ©lÃ©chargÃ© quotidiennement des documents sur Microsoftâ□□OneDrive, 7â□□% dans Google Gmail et 5â□□% dans Microsoft Sharepoint.

Cette hausse sensible du nombre dâ□□utilisateurs actifs sur un nombre record dâ□□applications cloud a entraÃ®nÃ© une augmentation considÃ©rable des tÃ©lÃ©chargements de malwares dans le cloud en 2022 par rapport Ã 2021, aprÃ¨s Ãªtre restÃ©s quasiment stables en 2021 par rapport Ã 2020.

La corrÃ©lation entre les tÃ©lÃ©chargements Ã destination et en provenance des applications les plus populaires nâ□□est pas une coÃ¯ncidence. PrÃ¨s dâ□□un tiers des tÃ©lÃ©chargements de logiciels malveillants dans le cloud provenait de Microsoft OneDrive, les plateformes Weebly et GitHub complÃ©tant le podium avec respectivement 8,6â□□% et 7,6â□□%.

Les malwares diffusÃ©s via le cloud, plus nombreux que ceux provenant du Web

Ces derniÃ¨res annÃ©es, les entreprises se sont de plus en plus appuyÃ©es sur des applications et lâ□□infrastructure cloud pour soutenir leur activitÃ© â□□ une tendance accÃ©lÃ©rÃ©e par la pandÃ©mie de COVID-19 et lâ□□avÃ¨nement des environnements de travail hybrides dans le monde entier. En consÃ©quence, les logiciels malveillants diffusÃ©s via le cloud sont dÃ©sormais responsables dâ□□un pourcentage plus Ã©levÃ© que jamais de malwares diffusÃ©s dans certaines rÃ©gions et certains secteurs dâ□□activitÃ©.

Entre 2021 et 2022, plusieurs rÃ©gions ont ainsi enregistrÃ© une hausse significative du pourcentage total de malwares dÃ©livrÃ©s via le cloud par rapport au Web, notammentâ□□:

â□¢ En Australieâ□□: 50â□□% en 2022 au lieu de 40â□□% en 2021
â□¢ En Europeâ□□: 42â□□% en 2022 au lieu de 31â□□% en 2021
â□¢ En Afriqueâ□□: 42â□□% en 2022 au lieu de 35â□□% en 2021
â□¢ En Asieâ□□: 45â□□% en 2022 au lieu de 39â□□% en 2021.

Dans certains secteurs, les logiciels malveillants dÃ©livrÃ©s via le cloud se sont Ã©galement imposÃ©s Ã lâ□□Ã©chelle mondialeâ□□:

â□¢ Dans les tÃ©lÃ©communicationsâ□□: 81â□□% en 2022 au lieu de 59â□□% en 2021
â□¢ Dans lâ□□industrie manufacturiÃ¨reâ□□: 36â□□% en 2022 au lieu de 17â□□% en 2021
â□¢ Dans la grande distributionâ□□: 57â□□% en 2022 au lieu de 47â□□% en 2021
â□¢ Dans la santÃ©â□□: 54â□□% en 2022 au lieu de 39â□□% en 2021.

Anticiper les cyber-risquesâ□□: le tÃ©lÃ©travail est lÃ pour durer

De nombreuses entreprises ont procÃ©dÃ© Ã des ajustements considÃ©rables en vue de faciliter la mise en place de lieux de travail Ã distance et hybrides. Si certains secteurs ont cherchÃ© Ã accÃ©lÃ©rer le retour des employÃ©s au bureau en 2022, les options de tÃ©lÃ©travail semblent largement rester en place.

Selon les donnÃ©es de ***Netskope***, laâ□□dispersion des utilisateurs - câ□□est-Ã -dire le rapport entre le nombre dâ□□utilisateurs de la plateforme Netskope et le nombre dâ□□emplacements rÃ©seau dâ□□oÃ¹ provient le trafic inhÃ©rent Ã ces utilisateurs - est de 66â□□%, soit le mÃªme quâ□□au dÃ©but de la pandÃ©mie voici plus de deux ans.

La dynamique du tÃ©lÃ©travail et du travail hybride continue de soulever de multiples dÃ©fis pour la cybersÃ©curitÃ©, quâ□□il sâ□□agisse de permettre aux utilisateurs dâ□□accÃ©der en toute sÃ©curitÃ© aux ressources dâ□□entreprise dont ils ont besoin pour accomplir leur travail, ou de leur fournir un accÃ¨s Ã©volutif et sÃ©curisÃ© Ã internet.

Netskope recommande aux entreprises de prendre les mesures suivantes pour Ã©viter toute augmentation des risques dâ□□incidents de sÃ©curitÃ© gÃ©nÃ©rÃ©s par les logiciels malveillants diffusÃ©s via le cloud et le Webâ□□:

â□¢ Mise en place de contrÃ´les de rÃ¨gles granulaires capables de limiter les flux de donnÃ©es en provenance et Ã destination des applications, professionnelles et personnelles, ou entre utilisateurs, ainsi quâ□□en provenance et Ã destination du Web, en adaptant les rÃ¨gles en fonction des appareils, des emplacements et des risques.

â□¢ DÃ©ploiement dâ□□une protection multicouches contre les menaces inline pour lâ□□ensemble du trafic provenant du cloud et du Web, dans le but de bloquer les communications entrantes et sortantes des logiciels malveillants.

â¢ Activation de lâauthentification multifacteur (MFA) pour les applications dâentreprise non managÃ©es.