Netskope : forte augmentation des tÃ©lÃ©chargements de phishing
Internet
PostÃ© par : JulieM
PubliÃ©e le : 11/5/2022 13:00:00

Netskope, leader du Security Service Edge (SSE) et du Zero Trust, publie une nouvelle Ã©tude qui rÃ©vÃ¨le que les tÃ©lÃ©chargements de phishing ont connu une trÃ¨s forte augmentation, Ã hauteur de 450 % au cours des 12 derniers mois.

Cette tendance est favorisÃ©e par lâutilisation de techniques dâoptimisation des moteurs de recherche (SEO) par les cybercriminels, dans le but dâamÃ©liorer le rÃ©fÃ©rencement de fichiers PDF malveillants sur les moteurs de recherche populaires, tels que Google et Bing. Ces PDF incluent notamment des faux CAPTCHA, qui redirigent les utilisateurs vers des sites de phishing, de spam, et dâescroquerie.

Les principales catÃ©gories de rÃ©fÃ©rencement web Ã©taient traditionnellement associÃ©es aux malwares, notamment les sharewares/freewares, mais Ã©taient dominÃ©es par des catÃ©gories moins conventionnelles. Ces conclusions figurent dans la derniÃ¨re Ã©dition du Â« Cloud and Threat Report: Global Cloud and Malware Trends Â» de Netskope, qui analyse les 12 derniers mois de tÃ©lÃ©chargements de malwares Ã partir du cloud et du web.

Le rapport rÃ©vÃ¨le que les cybercriminels mettent de plus en plus souvent en scÃ¨ne leurs attaques pour Ã©viter les filtres de geofencing et autres mesures de prÃ©vention traditionnelles. Ainsi, dâaprÃ¨s les conclusions du rapport, ils tendent Ã cibler les victimes situÃ©es dans une rÃ©gion spÃ©cifique au moyen de malwares hÃ©bergÃ©s dans cette mÃªme rÃ©gion.

De mÃªme, la pluralitÃ© de tÃ©lÃ©chargements de malwares a bien souvent pour origine la mÃªme rÃ©gion que la victime. Ce constat vaut tout particuliÃ¨rement pour lâAmÃ©rique du Nord, oÃ¹ 84 % de tous les tÃ©lÃ©chargements de malwares par des victimes nord-amÃ©ricaines ont Ã©tÃ© effectuÃ©s Ã partir de sites web hÃ©bergÃ©s en AmÃ©rique du Nord.

Â« Les malwares ne se limitent plus aux catÃ©gories traditionnelles de sites web Ã risque. Ils se tapissent dÃ©sormais partout, depuis les applications dans le cloud jusquâaux moteurs de recherche, exposant les entreprises Ã un risque plus Ã©levÃ© que jamais, analyse Ray Canzanese, directeur de la recherche sur les menaces chez Netskope.

Pour Ã©viter dâÃªtre victime de ces techniques dâingÃ©nierie sociale et de ces mÃ©thodes dâattaque ciblÃ©es, les responsables de la sÃ©curitÃ© doivent rÃ©guliÃ¨rement revoir leur stratÃ©gie de protection contre les malwares et veiller Ã ce que tous les points dâentrÃ©e potentiels soient couverts. Â»

Sur la base dâun sous-ensemble de donnÃ©es dâutilisation anonymes collectÃ©es par la plateforme Netskope Security Cloud, le rapport prÃ©sente dâautres conclusions importantes :

â¢ Les chevaux de Troie continuent de se montrer efficaces : les chevaux de Troie reprÃ©sentent 77 % de tous les tÃ©lÃ©chargements de malwares sur le web et dans le cloud, dans la mesure oÃ¹ les cybercriminels utilisent des techniques dâingÃ©nierie sociale pour sâimplanter et dÃ©livrer diverses charges utiles, notamment des portes dÃ©robÃ©es, des infostealers et des ransomwares.

Aucune famille de chevaux de Troie ne prÃ©domine Ã lâÃ©chelle mondiale. Les dix principales

familles de chevaux de Troie ne reprÃ©sentent que 13 % de tous les tÃ©lÃ©chargements, les 87 % restants rÃ©sultant de familles moins rÃ©pandues.

â¢ Le cloud et le web constituent le binÃ´me parfait pour un cybercriminel : 47 % des tÃ©lÃ©chargements de malwares proviennent dâapplications dans le cloud, contre 53 % de sites web traditionnels ; les hackers prÃ©fÃ©rant continuer Ã utiliser une combinaison de cloud et de web pour cibler leurs victimes.

â¢ Les applications de stockage dans le cloud les plus populaires continuent dâÃªtre Ã lâorigine de la plupart des tÃ©lÃ©chargements de malwares dans le cloud : parmi les autres principaux rÃ©fÃ©rencements dâapplications dans le cloud, citons celles de collaboration et de messagerie Web, grÃ¢ce auxquelles les hackers peuvent envoyer des messages directement Ã leurs victimes sous de multiples formes, notamment des emails, des messages directs, des commentaires et des partages de documents.

â¢ Les fichiers malveillants de Microsoft Office ont chutÃ© Ã des niveaux prÃ©-Emotet : les fichiers EXE et DLL reprÃ©sentent prÃ¨s de la moitiÃ© des tÃ©lÃ©chargements de malwares, les cybercriminels continuant Ã cibler Microsoft Windows, tandis que les fichiers Microsoft Office malveillants enregistrent une baisse et sont revenus aux niveaux antÃ©rieurs Ã Emotet.

Cela sâexplique en grande partie par les avertissements proactifs et les contrÃ´les de sÃ©curitÃ© mis en place lâannÃ©e derniÃ¨re par des fournisseurs de technologies comme Google et Microsoft.

Le Cloud and Threat Report de Netskope est Ã©ditÃ© par Netskope Threat Labs, une Ã©quipe de chercheurs spÃ©cialisÃ©s dans les menaces et les malwares liÃ©s au cloud, qui dÃ©tectent, analysent et conÃ§oivent des systÃ¨mes de protection contre les derniÃ¨res menaces liÃ©es au cloud et aux donnÃ©es qui affectent les entreprises.

Le Threat Research Hub de Netskop permet Ã la communautÃ© de la sÃ©curitÃ© dâaccÃ©der Ã davantage dâinformations, ainsi que dâÃ©changer et dâapprendre auprÃ¨s des chercheurs sur les menaces de Netskope et de la plateforme SSE intelligente de Netskope dÃ©diÃ© Ã lâÃ©volution du paysage des menaces dans le cloud.