Fausse MÃ J de Google, Danger.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 18/10/2023 13:00:00

Proofpoint Inc., sociÃ©tÃ© leader en matiÃ¨re de cybersÃ©curitÃ© et de conformitÃ©, publie les rÃ©sultats de sa derniÃ¨re Ã©tude rÃ©vÃ©lant une augmentation notable des fausses notifications de mise Ã jour navigateur. Une menace observÃ©e dans plusieurs pays dâ□□Europe dont la France.

Toutes les techniques sont bonnes pour abuser de la confiance des utilisateurs finaux. Et celle que nous plaÃ§ons presque aveuglÃ©ment envers les plateformes de services tels que Google Chrome ou Firefox, est une aubaine pour les cybercriminels qui parviennent aisÃ©ment Ã tromper leurs victimes grÃ¢ce Ã des techniques rodÃ©es dâ□□ingÃ©nierie sociale.

Ã□tes-vous sÃ»r que votre navigateur est Ã jourâ□□?

Ces Â«â□□attaquesâ□□Â» apparaissent sur des sites web dÃ©jÃ compromis et prennent la forme dâ□□une alerte venant directement du navigateur utilisÃ©, qui peut Ãªtre Google Chrome, Firefox ou encore Edge. Ces notifications dâ□□apparence familiÃ¨re indiquent que le navigateur en question nÃ©cessite dâ□□Ãªtre mis Ã jour, invitant lâ□□utilisateur Ã cliquer sur un lien de tÃ©lÃ©chargement qui, sans le savoir, cache un logiciel malveillant.

Le plus souvent en anglais, on observe cette fois-ci des attaques en franÃ§ais, en espagnol, en allemand et en portugais.

Figure 1 : capture dâ□□Ã©cran saisi pas la Threat Research team de Proofpoint

DÃ©jÃ utilisÃ©e par TA569 pour diffuser le logiciel malveillant SocGolish, Proofpoint a rÃ©cemment identifiÃ© de nouveaux groupes ayant adoptÃ© cette mÃ©thode dont : RogueRaticate, SmartApeSG et ClearFake. Si chacun dÃ©ploie ses propres campagnes pour diffuser leurs piÃ¨ges sous forme de notification frauduleuse, celles-ci prÃ©sentent des caractÃ©ristiques communes qui suivent un mÃªme schÃ©ma.

Figure 2 : chaÃ®ne dâ□□attaque identifiÃ©e par Proofpoint

Les chercheurs de chez Proofpoint expliquent, Â«â□□nous avons identifiÃ© une augmentation du nombre dâ□□acteurs utilisant cette technique de fausse mise Ã jour pour tromper les utilisateurs finaux et les inciter Ã tÃ©lÃ©charger leur logiciel infectÃ©.

Une forme dâ□□attaque unique, qui associe technicitÃ© et ingÃ©nierie sociale pour rÃ©ussir Ã convaincre leurs cibles de lâ□□authenticitÃ© du message. Bien quâ□□elle ressurgisse actuellement, cette technique nâ□□est pas nouvelle et a dÃ©jÃ Ã©tÃ© adaptÃ©e Ã dâ□□autres logiciels malveillants dans le but de voler des donnÃ©es, accÃ©der au contrÃ´le Ã distance dâ□□un ordinateur ou mÃªme pour les ranÃ§ongiciels.â□□Â»

Cette technique sâ□□avÃ¨re particuliÃ¨rement efficace, car elle exploite des enseignements tirÃ©s des formations en cybersÃ©curitÃ© qui incitent les utilisateurs Ã nâ□□accepter les mises Ã jour que de sites connus et fiables.

En compromettant ces sites de confiance et grÃ¢ce Ã des techniques de vÃ©rification discrÃ¨tes,

les leurres passent inaperÃ§us. Une rÃ©ussite qui souligne la difficultÃ© quâ□□ont les Ã©quipes de sÃ©curitÃ© Ã dÃ©tecter, prÃ©venir et surtout bien communiquer le risque chronique auquel les utilisateurs finaux sont exposÃ©s.

Â«â□□Cette recrudescence sâ□□explique notamment par son efficacitÃ©, car les acteurs de la menace exploitent la volontÃ© des utilisateurs de bien faire. En voulant sÃ©curiser leur environnement de travail et protÃ©ger leurs informations, ils font finalement lâ□□inverse et sâ□□exposent aux risques dâ□□infection et de propagation dâ□□un logiciel malveillantâ□□Â» prÃ©cisent les chercheurs de chez Proofpoint.

Quels conseils pour pallier ce risque ?

Face Ã cette menace croissante, la meilleure solution reste encore la dÃ©fense en profondeur. Les organisations doivent mettre en place des systÃ¨mes de dÃ©tection en rÃ©seau et protÃ©ger les points dâ□□accÃ¨s. Bien quâ□□elle ne soit pas infaillible, une formation spÃ©cifique et de la prÃ©vention sont Ã©galement vitales pour permettre aux utilisateurs dâ□□Ãªtre en capacitÃ©, justement, dâ□□identifier ce type dâ□□activitÃ©s suspectes et de les signaler aux Ã©quipes de sÃ©curitÃ©.

Vous trouverez lâ□□intÃ©gralitÃ© de cette recherche sur le site de Proofpoint :Â