Les cybercriminels changent constamment leurs méthodes de distribution de fichiers malveillants et incitent les utilisateurs à télécharger des logiciels malveillants comme des chevaux de Troie. La nouvelle campagne exploite de faux bugs dans les navigateurs Google Chrome, Word et OneDrive pour tromper les utilisateurs.

Observée par plusieurs cybercriminels, dont certains sont connus pour leurs campagnes de distribution massive de spam par courrier électronique, cette campagne utilise des messages d'erreur envoyés par courrier électronique et des superpositions de sites Web pour inciter les utilisateurs à télécharger de fausses mises à jour de navigateur. Ces mises à jour installent ensuite des logiciels malveillants sur l'appareil de l'utilisateur.

Plusieurs personnes ont identifié trois types d'attaque pour diffuser les malwares :

-Faux avertissements de Google Chrome : ces messages apparaissent lorsqu'un utilisateur visite un site Web compromis et demande d'installer un « certificat racine » en copiant un script PowerShell et en l'exécutant dans la console d'administration Windows. Ce script affiche des messages factices tout en téléchargeant et installant un malware voleur d'informations.

-Superpositions d'erreurs de Google Chrome : Utilisées sur des sites web compromis pour afficher de fausses erreurs.

-Faux e-mails d'erreur Word : les utilisateurs reçoivent des e-mails ressemblant à des messages Microsoft Word, les incitant à télécharger de fausses extensions "Word Online" pour afficher des documents. Ces messages d'erreur contiennent des offres de « réparation automatique » qui téléchargent des logiciels malveillants lorsqu'ils sont copiés et collés dans PowerShell.

Cette campagne repose sur le manque de sensibilisation des utilisateurs et l'incapacité de Windows à détecter et bloquer ces actions malveillantes, aggravant ainsi le problème de sécurité.

Sources : thehindu.com