Arnaque aux places de concert via des Call-centers.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 10/11/2021 15:00:00

Les chercheurs de Proofpoint ont observÃ© une augmentation des menaces perpÃ©trÃ©es via des call-centers.

Via un solide Ã©cosystÃ¨me de menaces par e-mail, ces attaques reposent sur le fait que les victimes appellent directement les attaquants et initient l'interaction. Cette fraude est prolifique et rentable : dans de nombreux cas, les victimes perdent des dizaines de milliers dâeuros volÃ©s (allant jusquâÃ 50 000 par attaque si ce nâest plus) directement sur leur compte bancaire.

Deux types d'activitÃ©s menaÃ§antes sont rÃ©guliÃ¨rement observÃ©s par Proofpoint. L'une met en scÃ¨ne la fraude traditionnelle des call-centers en proposant une fausse assistance technique et ainsi voler de lâargent. La seconde exploite l'utilisation d'un logiciel malveillant pour compromettre un ordinateur.

Cette derniÃ¨re est frÃ©quemment associÃ©e au malware BazaLoader et est souvent appelÃ© BazaCall. Les deux types menaces sont ce que Proofpoint considÃ¨re comme des attaques par tÃ©lÃ©phone aussi nommÃ©es TOAD (telephone-oriented attack delivery).

Les thÃ¨mes liÃ©s Ã la culture populaire sont majoritairement privilÃ©giÃ©s. Parmi les attaques les plus rÃ©centes, les acteurs de la menace envoient des emails Ã une victime en prÃ©tendant Ãªtre des vendeurs de billets pour The Weeknd ou Justin Bieber, des services de sÃ©curitÃ© informatique, des organismes liÃ©s au COVID-19 ou des sites de vente en ligne, promettant des remboursements pour des achats erronÃ©s, des mises Ã jour de logiciels ou un soutien financier.

Ces e-mails contiennent un numÃ©ro de tÃ©lÃ©phone pour l'assistance clientÃ¨le. Lorsque les victimes appellent le numÃ©ro pour obtenir de l'aide, elles sont directement mises en relation avec un tÃ©lÃ©conseiller qui sâavÃ¨re Ãªtre finalement un hacker.

Chaque jour Proofpoint dÃ©tecte et bloque des dizaines de milliers de menaces par e-mail par tÃ©lÃ©phone. Les chercheurs ont retrouvÃ© les auteurs de ces menaces dans plusieurs zones d'opÃ©rations et, grÃ¢ce aux donnÃ©es des emails, aux conversations tÃ©lÃ©phoniques et aux messages, ils sont maintenant en mesure de fournir un aperÃ§u exclusif de la maniÃ¨re dont le secteur florissant des call centers est devenu la cible de nombreuses menaces.

Selon Sherrod DeGrippo, Directrice menaces Ã©mergentes chez Proofpoint Â« Les acteurs de la menace font preuve d'une grande crÃ©ativitÃ© dans leurs appÃ¢ts, et un faux reÃ§u pour des billets pour Justin Bieber ou le remboursement dâun achat en ligne sont suffisamment accrocheurs pour tromper par e-mail mÃªme le plus vigilant des destinataires.

Si vous rÃ©pondez pour tenter de contester les frais, s'ensuit alors une succession dâinfections toutes plus Ã©laborÃ©es les unes que les autres, nÃ©cessitant une interaction humaine importante et entraÃ®nant les victimes vers une immense arnaque. Ces fausses plateformes de service client finissent par leur dÃ©rober de lâargent Ã leur victime ou propager des infections par logiciel malveillant. Â»

Pour en savoir plus sur ces menaces liÃ©es Ã des phÃ©nomÃ¨nes grand public.