Ponemon Institute : CoÃ»ts du phishing,14,8M de dollars par an
Internet
PostÃ© par : JulieM
PubliÃ©e le : 23/8/2021 13:00:00

Proofpoint, Inc. (NASDAQ : PFPT), sociÃ©tÃ© leader en cybersÃ©curitÃ© et en conformitÃ©, et Ponemon Institute, l'un des principaux organismes de recherche en sÃ©curitÃ© informatique, publient aujourd'hui les rÃ©sultats d'une nouvelle Ã©tude sur le coÃ»t des attaques de phishing.

Le rapport rÃ©vÃ¨le que le coÃ»t a presque quadruplÃ© au cours des six derniÃ¨res annÃ©es, les grandes entreprises amÃ©ricaines perdant en moyenne 14,8 millions de dollars par an (soit 1 500 dollars par employÃ©), un chiffre en forte hausse par rapport aux 3,8 millions de dollars enregistrÃ©s en 2015.

Selon l'Ã©tude, qui a interrogÃ© prÃ¨s de 600 experts IT et de la sÃ©curitÃ© informatique, les menaces les plus coÃ»teuses pour les entreprises sont les attaques de type BEC et par ranÃ§ongiciels. Mais les coÃ»ts pour les organisations vont bien au-delÃ des fonds transfÃ©rÃ©s aux attaquants.

Â« Lorsqu'une organisation paye des millions pour rÃ©soudre une attaque par ranÃ§ongiciels, la plupart des personnes supposent que la rÃ©solution du problÃ¨me a coÃ»tÃ© Ã l'entreprise la ranÃ§on uniquement. Or, nous avons constatÃ© que la ranÃ§on seule reprÃ©sente moins de 20 % du coÃ»t d'une attaque par ranÃ§ongiciel Â», dÃ©clare Larry Ponemon, prÃ©sident et fondateur du Ponemon Institute.

Â« Comme les attaques de phishing augmentent la probabilitÃ© d'une violation des donnÃ©es et d'une perturbation de l'activitÃ©, la plupart des coÃ»ts encourus par les entreprises proviennent de la perte de productivitÃ© et de la remÃ©diation du problÃ¨me plutÃ´t que de la ranÃ§on rÃ©elle versÃ©e aux attaquants. Â»

La compromission dâ□□identifiants prÃ©cÃ¨de gÃ©nÃ©ralement les attaques de type BEC et par ranÃ§ongiciels, gÃ©nÃ©ralement sous la forme d'un employÃ© qui se fait piÃ©ger pour donner ses informations d'identification. Selon l'Anti-Phishing Working Group (APWG), le phishing est un crime qui fait appel Ã l'ingÃ©nierie sociale et Ã des subterfuges techniques pour voler des informations personnelles et des identifiants de comptes financiers.

La croissance du phishing n'est pas progressive - elle est exponentielle, l'APWG estimant que les attaques de phishing ont doublÃ© rien qu'en 2020.

Voici d'autres conclusions clÃ©s du rapport 2021 sur le coÃ»t du phishing :

â□¢ La perte de productivitÃ© est l'un des rÃ©sultats les plus coÃ»teux des attaques de phishing. Dans une entreprise amÃ©ricaine de taille moyenne de 9 567 personnes, cela se traduit par 63 343 heures perdues chaque annÃ©e. Chaque employÃ© perd en moyenne sept heures par an Ã cause des escroqueries par phishing, soit une augmentation par rapport aux quatre heures de 2015.

â□¢ Les attaques de compromission dâ□□emails professionnels (BEC) coÃ»tent prÃ¨s de 6 millions de dollars par an aux grandes entreprises. Sur ce montant, les paiements illicites versÃ©s chaque annÃ©e aux attaquants de ce type dâ□□attaque reprÃ©sentent 1,17 million de dollars.

â□¢ Les ranÃ§ongiciels coÃ»tent 5,66 millions de dollars par an aux grandes entreprises. Sur ce

montant, 790 000 dollars correspondent aux ranÃ§ons payÃ©es.

â¢ La formation de sensibilisation Ã la sÃ©curitÃ© rÃ©duit les dÃ©penses liÃ©es au phishing de plus de 50 % en moyenne.

â¢ Les coÃ»ts de rÃ©solution des infections par logiciels malveillants ont plus que doublÃ© depuis 2015. Le coÃ»t total moyen pour rÃ©soudre les attaques de logiciels malveillants s'Ã©lÃ¨ve Ã 807 506 dollars en 2021, soit une augmentation par rapport aux 338 098 dollars de 2015.

â¢ Les coÃ»ts liÃ©s Ã la compromission dâidentifiants ont augmentÃ© de faÃ§on spectaculaire depuis 2015. Par consÃ©quent, les organisations dÃ©pensent davantage pour rÃ©pondre Ã ces attaques. Le coÃ»t moyen pour contenir les compromissions dâidentifiants basÃ©es sur le phishing est passÃ© de 381 920 dollars en 2015 Ã 692 531 dollars en 2021. Les organisations ont subi en moyenne 5,3 compromissions sur une pÃ©riode de 12 mois.

â¢ Les chefs d'entreprise doivent prÃªter attention aux scÃ©narios de pertes maximales probables. Par exemple, les attaques BEC pourraient entraÃ®ner des pertes pouvant atteindre 157 millions de dollars si les organisations ne sont pas prÃ©parÃ©es. Les logiciels malveillants entraÃ®nant l'exfiltration de donnÃ©es pourraient coÃ»ter aux entreprises jusqu'Ã 137 millions de dollars.

Â« Parce que les acteurs de la menace ciblent dÃ©sormais les employÃ©s plutÃ´t que les infrastructures, la compromission dâidentifiants a explosÃ© ces derniÃ¨res annÃ©es, laissant la porte grande ouverte Ã des attaques beaucoup plus dÃ©vastatrices comme les attaques de type BEC ou par ranÃ§ongiciels Â», a dÃ©clarÃ© Ryan Kalember, vice-prÃ©sident exÃ©cutif de la stratÃ©gie de cybersÃ©curitÃ© chez Proofpoint.

Â« Tant que les organisations ne dÃ©ploieront pas une approche de la cybersÃ©curitÃ© centrÃ©e sur l'humain, comprenant une formation Ã la sensibilisation Ã la sÃ©curitÃ© et une protection intÃ©grÃ©e contre les menaces pour les arrÃªter et y remÃ©dier, les attaques de phishing se poursuivront. Â»

Pour tÃ©lÃ©charger le rapport Ponemon sur le coÃ»t des menaces phishing 2021.

Pour plus d'informations sur les solutions de phishing entiÃ¨rement intÃ©grÃ©es de Proofpoint :.