Des annonces dâ□□emplois frauduleuses diffusÃ©es sur les RS
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/3/2023 14:00:00

Depuis quelques mois, des annonces dâ□□emplois frauduleuses diffusÃ©es sur des plateformes populaires telles que LinkedIn, Indeed et Monsters, piÃ¨gent un nombre croissant de demandeurs dâ□□emploi.

Dans une nouvelle recherche, les chercheurs du Advanced Research Center de Trellix rÃ©vÃ¨lent quelles sont les tactiques les plus utilisÃ©es par les cybercriminels pour mener Ã bien ce type dâ□□escroquerie :

â□¢ Des sites frauduleux

Les cybercriminels crÃ©ent des domaines web qui ressemblent aux sites web lÃ©gitimes, mais avec des lÃ©gÃ¨res variations, telles que des mots mal orthographiÃ©s ou des extensions diffÃ©rentes.

Voici quelques exemples de domaines frauduleux observÃ©s par Trellix : indeed-id.com, indeed-7.com, indeed-a.com, indeed.ch, indedd.com, linkhedin.com, linkegin.com, linkednn.com

â□¢ Des e-mails phishing

Les e-mails se prÃ©sentent sous la forme d'une notification d'offre d'emploi qui contient une URL ou une piÃ¨ce jointe, dirigeant la victime vers une page de phishing ou tÃ©lÃ©chargeant un malware sur son systÃ¨me.

â□¢ Des URLs malveillants et des Malwares

Les cybercriminels utilisent des pages web malveillantes conÃ§ues pour imiter les formulaires de connexion des sites dâ□□emploi, afin de tromper les utilisateurs et de rÃ©cupÃ©rer leurs informations personnelles. En outre, plusieurs familles de logiciels frauduleux ont Ã©tÃ© identifiÃ©es.

Cette Ã©tude soulÃ¨ve des graves prÃ©occupations quant Ã la sÃ©curitÃ© des donnÃ©es personnelles des utilisateurs sur les plateformes de recherche dâ□□emploi en ligne, car ce type dâ□□escroquerie est en constante Ã©volution, avec des nouveaux stratagÃ¨mes qui apparaissent rÃ©guliÃ¨rement.

Il est essentiel se munir dâ□□outils efficaces, tels que lâ□□XDR, afin de protÃ©ger les utilisateurs de toute forme de cybermenace.

Advanced Research Center de Trellix.