Les relations sentimentales populaires auprÃ¨s des pirates.
Internet
PostÃ© par : JPilo
PubliÃ©e le : 10/2/2023 14:00:00

A l'occasion de la Saint Valentin, Matthew Psencik, Director Endpoint Security chez Tanium, nous explique pourquoi les escroqueries autour des relations sentimentales sont si populaires auprÃ¨s des pirates.

Pourquoi les escroqueries autour de l'amour et des relations sentimentales sont-elles populaires ?

"Les escroqueries Ã caractÃ¨re romantique sont populaires parce qu'elles touchent des cordes sensibles. Les gens sont moins mÃ©fiants lorsqu'il s'agit d'amour et de relations, et baissent souvent leur garde alors qu'ils seraient beaucoup plus prudents dans une autre situation.

Ces attaques, qui relÃ¨vent gÃ©nÃ©ralement du domaine de l'ingÃ©nierie sociale (c'est Ã dire qu'elles visent Ã dÃ©clÃ©ncher une action prÃ©cise de la part de son destinataire), mettent l'accent sur la vulnÃ©rabilitÃ© en exerÃ§ant une pression sur une personne pour lui donner un sentiment d'urgence ou en la dÃ©tournant de toute pensÃ©e rationnelle.

Et la collecte d'informations pour identifier et exploiter la cible visÃ©e est plus facile que jamais pour les cybercriminels. Les applications de rencontres et les profils des mÃ©dias sociaux regorgent de dÃ©tails intimes sur la vie d'une personne.

Les internautes publient sans sans rendre compte un grand nombre de donnÃ©es trÃ¨s intÃ©ressantes pour les cybercriminels : le statut d'une relation, la profession, les loisirs, les photos personnelles et parfois les numÃ©ros de tÃ©lÃ©phone ou les adresses.

Ces informations permettent aux cybercriminels, soit de crÃ©er manuellement de faux profils attrayants et d'entrer en contact avec des utilisateurs cibles, soit de crÃ©er des robots qui se chargeront de l'ensemble du cycle d'attaque Ã leur place.

Une fois qu'un attaquant a trouvÃ© une victime potentielle, il peut tenter d'obtenir des informations personnelles par le biais d'une usurpation d'identitÃ© ou des gains monÃ©taires par le biais du chantage. Dans certains cas, il peut mÃªme partager des liens malveillants pour lancer toute une sÃ©rie d'autres attaques."

Quelles sont les attaques les plus courantes ?

"Les cybercriminels optent pour ce qui fonctionne. Les escroqueries romantiques ne font pas exception Ã la rÃ¨gle et s'appuient gÃ©nÃ©ralement sur des techniques Ã©prouvÃ©es de phishing et de spear phishing.

Elles visent Ã duper les victimes pour qu'elles rÃ©vÃ¨lent des informations personnelles telles que le nom de leur animal de compagnie, qui est une question de sÃ©curitÃ© frÃ©quente sur les sites web, et des numÃ©ros de tÃ©lÃ©phone qui permettent de suivre et de localiser plus facilement une personne.

Cependant, les possibilitÃ©s d'extorsion, de chantage et d'autres fraudes sont bien plus insidieuses lorsqu'il s'agit d'une relation amoureuse, impliquant souvent des images ou des vidÃ©os explicites,

ainsi que des demandes de fonds importants pour des dÃ©placements et des dÃ©penses en vue d'une rencontre qui n'aura jamais lieu, etc."

Quels sont les signes d'une Ã©ventuelle de ce type d'escroquerie ?

"Si quelque chose vous semble anormal, c'est probablement le cas. Une diction, une orthographe et une structure de phrase Ã©tranges devraient immÃ©diatement vous alerter et vous faire penser que vous avez affaire Ã quelque chose de malveillant, comme un robot ou un autre programme d'Intelligence Artificielle.

Si une personne est trop directe ou trop personnelle sans aucune interaction au prÃ©alable, posez-lui une question personnelle assez complexe. Cela permettra de briser les tentatives d'un robot de suivre un script ou obligera l'escroc Ã essayer de ramener la conversation vers son objectif.

MÃ©fiez-vous Ã©galement des demandes d'aide ou d'argent qui sortent de nulle part. Les demandes de fonds par des moyens inhabituels, tels que les demandes multiples de cartes-cadeaux ou les transferts de bitcoins, doivent susciter l'inquiÃ©tude et donner lieu Ã une rÃ©flexion plus approfondie.

En ce qui concerne ce type d'escroqueries, soyez conscient que les applications de rencontre regorgent de bots et d'escrocs, ce qui fait que vous avez de fortes chances d'Ãªtre confrontÃ© Ã l'un ou l'autre.

Si vous pensez Ãªtre une cible, assurez-vous de "blacklister" cette "personne" dÃ¨s que possible. Et si vous voulez contribuer Ã l'amÃ©lioration de ces plateformes, faites un rapport et laissez l'Ã©quipe de modÃ©ration de l'application prendre le relais."