Así funciona la estafa en aplicaciones de redes sociales y criptomonedas

29/10/2022

Los **cibercriminales** inventan constantemente nuevas formas de encontrar fallas de seguridad que les permitan beneficiarse de las **vulnerabilidades** en los dispositivos y la confianza de los usuarios. Las **aplicaciones de citas** y las de **redes sociales** son algunas de las plataformas más usadas por estos delincuentes para realizar estafas y robar el dinero de las personas.

En los últimos meses se han reportado algunos casos de **Pig Butchering**, una nueva modalidad de **engaño** por internet en el que se usan estas aplicaciones que prometen romances virtuales para iniciar a los usuarios a comprar **criptomonedas**, a diferencia de otras formas en las que solo se finge un **interés romántico**, como en el Romance Scam, para que la víctima

realice **transferencias** bancarias a favor del **delincuente**.

La estafa del **Pig Butchering**, que tiene origen chino, se ha posicionado como una modalidad de ciberataque de ingeniería social que ha afectado a miles de personas y ha generado una pérdida de **122.00 dólares** a los usuarios víctimas de esta estafa. Además, como dato adicional, dos tercios de las personas afectadas son **mujeres** con edades entre **25 y 44 años de edad**.

Los usuarios víctimas de Pig Butchering son invitados constantemente a realizar inversiones en criptomonedas. REUTERS/Edgar Su

Cómo funciona la estafa en las aplicaciones de citas

La empresa de **ciberseguridad** Proofpoint, que realizó el estudio que detectó la estafa, indica que los delincuentes inician el contacto con sus **víctimas** por medio de redes

sociales con excusas para mantener la conversación activa.

Una vez que se obtiene una respuesta positiva por parte del usuario, los **ciberdelincuentes** comienzan a enviar fotos y a desarrollar un **diálogo** con la intención de **seducir** y ganar la **confianza** de sus víctimas aportando cierto nivel de realidad.

Con el tiempo, los atacantes indican tener un amigo o pariente que les ha ayudado a viajar a otros países y, con ánimos de tener una **conversación** más privada, sugieren continuar el dialogo en plataformas de mensajería como **Telegram** o **WhatsApp**.

Una vez que la víctima ha brindado su número de **teléfono** y que las conversaciones incluyen fotos sugerentes, se vuelve a nombrar a a persona que ha "solucionado sus problemas económicos" y ofrece la posibilidad de **ganar dinero** de forma sencilla por medio de una inversión en **criptomonedas**.

Una vez agotado el dinero de las víctimas, los cibercriminales cierran el sitio web y el dominio utilizado se reinicia con un nombre distinto para seguir estafando a otras personas. (foto: CriptoNoticias)

Las víctimas entonces son saturadas con invitaciones a **grupos de chat** en aplicaciones de **mensajería** en los que se habla

sobre los beneficios de invertir en **criptomonedas**. El resto de personas incluidas en estos colectivos **virtuales** también son atacantes quienes afirman que se han visto beneficiados por sus **inversiones**.

Debido a la insistencia, si la potencial **víctima** decide comprar una pequeña cantidad de criptomonedas, los ciberdelincuentes indican que para ver **mayores beneficios** realicen gastos inferiores a **1.000 dólares**, monto que aumentará de forma progresiva

En el caso de que las personas decidan dejar de **invertir** por falta de **dinero**, estas son incentivadas a solicitar préstamos, hipotecar sus viviendas o vender acciones. Si la víctima se niega, entonces los **ciberdelincuentes** explicarán que no pueden retirar todo el dinero acumulado y, si insisten en no realizar más **inversiones**, **amenazan** a las **víctimas** con denunciarlas por fraude o **evasión de impuestos** usando capturas de pantalla de estados de cuenta de la criptomoneda.

Finalmente, una vez que el cibercriminal inicia el **retiro del dinero** de los usuarios, se elimina el dominio del sitio web en el que se realizó la inversión, se **bloquea** a la víctima de la aplicación de mensajes. Los **perfiles** son configurados para llegar a afectar a más personas y las víctimas no tienen otra **opción** para **reportar** el problema.

Fuente: Infobae