CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Estafa Cibernética

Fecha: **10/10/2022**

Problemática: **Ciberataques a través del chatbot de Messenger de Facebook Meta**

Correlativo: **AA-0034**

Institución / Sector: **Público en General**

CONTEXTO

Panda Security lanzó un comunicado por medio de sus canales oficiales informando al público en general sobre una técnica de ingeniería social utilizada por ciberdelincuentes para hacerse de las credenciales de su víctima en torno a páginas de Facebook y el Messenger de Facebook Meta.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
No Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Medio	**Baja**	**Baja**	**Media**

SITUACIÓN

Haciendo uso de técnicas de ingeniería social, ciberdelincuentes engañan a sus víctimas, haciéndose pasar por el equipo de soporte técnico de Facebook Meta. De acuerdo a la investigación realizada por el Centro Estratégico de Monitoreo -CEM, el objetivo de los ciberdelincuentes es claro," Robar las credenciales de inicio de sesión de Facebook". La estafa se lleva a cabo de la siguiente manera:

- **Comienza con un correo electrónico de phishing, cuyo titular y cuerpo del mensaje informan sobre la necesidad de ponerse en contacto con el equipo de soporte de Facebook.**
- **El correo proporciona un enlace para "apelar" redirige a su víctima a una conversación de Messenger con un chatbot, que de nuevo les ofrece otro enlace, como si se tratase de un servicio de soporte técnico.**
- **Acto seguido, la falsa página de soporte, pone a disposición de la víctima un formulario que debe rellenar con datos personales como número de teléfono, su perfil o página de Facebook que pretenden mantener y pulsar a "Enviar", cuyo paso final pasa por pedirles la contraseña de su Facebook.**
- **Una vez se han insertado el código numérico de la autenticación, que se habrá enviado a través de SMS, la página redirige a una página real del centro de ayuda de Facebook.**
- **El hecho de que pongan una página real de Facebook sobre pautas relacionados con violaciones sobre contenido por parte del usuario y propiedad intelectual pone el broche de oro al engaño, proporcionándole más veracidad a la estafa"**

RECOMENDACIONES

El Centró Estratégico de Monitoreo-CEM recomienda a los internautas guatemaltecos a que no se dejen engañar por este tipo de estas de ingeniería social, por lo que enfatizamos en lo siguiente:

- **Analizar el encabezado del correo electrónico y verificar el dominio del remitente (Facebook).**
- **Comprobar la URL del sitio o página web que visitamos y comprobar si el dominio corresponde con el original, en este caso de Facebook, para evitar acceder con nuestras cuentas a sitios fraudulentos.**

Tomar la precaución del caso, y, en especial, cuando se trata de ciberataques con técnicas de ingeniería artificial avanzadas como la expuesta en esta alerta.

DICCIONARIO DE DATOS

1. **Phishing: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario.**
2. **Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo,**
3. **Chatobot: Software que simulan mantener una conversación con una persona al proveer respuestas automáticas, las cuales son previamente establecidas por un conjunto de expertos a entradas realizadas por el usuario.**
4. **Ingeniería social: Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.**
5. **Ingeniería artificial: combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.**

REFERENCIAS

1. **https://www.pandasecurity.com/es/mediacenter/redes-sociales/ciberataque-messenger-meta/**
2. **https://www.virustotal.com/gui/home/url**

ÁREA PARA DEFINICIONES

*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.