Las ‘estafas del amor’ le cuestan hasta 1,300 millones de dólares a las empresas en San Valentín

- *Engaños mediante apps de citas y tarjetas de regalo falsas son solo ejemplos de formas que los cibercriminales utilizan para propagar amenazas.*

CIUDAD DE MÉXICO. 14 de febrero de 2024.- Según el reciente informe de Netskope "Year in Review, Cloud and Threat Report”, la forma más común en que los ciberdelincuentes accedieron a las distintas organizaciones en 2023 fue a través de la ingeniería social. Aunque es una de las tácticas favoritas de los criminales informáticos, la ingeniería social no consiste simplemente en descifrar código mientras se está encima de un teclado. Utiliza la propia debilidad del individuo, animando a las víctimas a abrir la puerta al atacante.

Para Paolo Passeri de Netskope, San Valentín es una buena oportunidad para que los ciberdelincuentes se aprovechen de la situación de vulnerabilidad de sus objetivos en estas fechas y, en última instancia, llegar hasta las empresas:

Identificar los puntos débiles

Aunque la mayoría de las personas piensa que nunca sería víctima de este tipo de ataques, lo cierto es que todos podemos sufrirlos. Cualquiera que se deje llevar por sus emociones puede fácilmente cometer errores de seguridad, dar acceso no autorizado a información sensible o incluso ser él mismo quien divulgue información sensible.

San Valentín es un buen ejemplo. Las estafas románticas son un negocio redondo, con un volumen de daños a las víctimas que alcanzó los 1,300 millones de dólares en años anteriores en mercados de referencia como Estados Unidos; y los 92.8 millones de libras en el Reino Unido en 2023. Los casos de fraude no se limitan al 14 de febrero, pero es cuando las víctimas son más vulnerables. La prensa nos regala periódicamente ejemplos de estafadores del amor que suplantan perfiles falsos en las redes.

Alguien que busca el amor puede ser lo suficientemente inteligente como para ignorar los mensajes no solicitados de un perfil de citas falso 364 días al año, pero si la fiebre de San Valentín le ha hecho sentirse especialmente solo o sola, puede sentirse más inclinado a responder. Del mismo modo, los que ya tienen pareja pueden encontrarse en un estado de ánimo diferente cuando se acerca San Valentín, por ejemplo, con ganas de celebrar un momento importante de la relación o ser objeto de una invitación sorpresa. En ese caso, es más probable que hagan clic en una oferta de tarjeta regalo de 100 euros sin comprobar antes que procede de una fuente legítima.

Aunque el amor, la soledad y la ilusión son emociones fácilmente reconocibles de las que se puede sacar provecho, cualquier situación que afecte a la vida emocional de una persona puede hacerla vulnerable.

Controlar el riesgo

Las organizaciones pueden defenderse de estos ataques de muchas maneras. El riesgo aumenta inevitablemente con el uso de aplicaciones no empresariales en los dispositivos corporativos, por lo que algunas pueden optar por políticas que bloqueen completamente el acceso a apps personales -como las de citas- en sus dispositivos. El ascenso de la inteligencia artificial, por ejemplo, ha llevado a muchas empresas a considerar la posibilidad de bloquear herramientas como ChatGPT y la inteligencia artificial generativa en sus sistemas. Sin embargo,

el simple bloqueo de todas las aplicaciones no empresariales puede crear frustración, limitar la innovación y dar la impresión de falta de confianza en el personal.

En su lugar, las empresas pueden aplicar un enfoque menos radical que se base en herramientas inteligentes, así como en equipos de seguridad que analicen de forma rutinaria el tráfico HTTP/HTTPS, con un criterio más ágil que se traslade a la nube, según una arquitectura de paso único. También pueden implementarse controles de seguridad más estrictos, como el agente de seguridad de acceso a la nube (CASB), la pasarela web segura (SWG), la prevención de amenazas y de pérdida de datos (DLP).

También deben centrarse en la sensibilización y la educación, entrenando a los usuarios a ser vigilantes antes de hacer clic en un enlace o acceder a una aplicación no autorizada. Para ayudar a los usuarios a que comprendan su propia vulnerabilidad, es importante centrarse en los riesgos personales, no sólo en el impacto sobre la empresa. Utilizar ejemplos de cómo los ataques pueden afectar -y derivarse- de la vida personal de las personas puede ayudarles a comprender mejor cómo pueden convertirse en objetivo.

Fomentar la colaboración

Con independencia de lo que decida hacer una organización, es imposible evitar que los empleados pinchen en un enlace malicioso, y el mayor riesgo suele producirse cuando los usuarios esconden un incidente de seguridad en Internet, sobre todo si se trata de un ataque de ingeniería social en el que pueden llegar a sentirse personalmente responsables.

En caso de verse comprometido, es esencial reducir el tiempo necesario para mitigar el ataque, por eso no se debe culpar a las víctimas de los ataques, es el camino equivocado. La clave está en fomentar una cultura de colaboración en la que los empleados formen parte activa del proceso, en lugar de inculcar una cultura del miedo. Concienciar a la plantilla en un clima de colaboración puede contribuir en gran medida a reducir el riesgo de que los ciberdelincuentes se aprovechen de que los seres humanos son débiles, sobre todo en fechas como San Valentín.

Para saber más sobre la investigación de Netskope Threat Labs sobre amenazas en la nube como la que supone la ingeniería social, lee nuestro último Informe sobre “Cloud and Threat Report , 2023 Year in Review".

###