Y por si fuera poco, ahora también hay que tener cuidado con LinkedIn

01/05/2022

Check Point Research, una de las empresas líder en soluciones de seguridad cibernética a nivel mundial, publicó el primer informe sobre phishing de marca de 2022, correspondiente al primer trimestre del año. Este trabajo recopila información de todo el mundo y elabora un ranking de las marcas que fueron imitadas con mayor frecuencia por ciberdelincuentes en sus intentos de robar la información personal o las credenciales de pago de los usuarios.

Los datos para este trimestre son muy llamativos y están relacionados con LinkedIn. Por primera vez desde que Check Point Research publica sus informes trimestrales sobre phishing, esta red social fue la marca más utilizada por los ciberdelincuentes para el robo de datos y representó el 52% de todos los intentos de phishing del trimestre.

El crecimiento de LinkedIn en relación al trimestre anterior

es espectacular. Alcanza con decir que durante ese lapso, es decir octubre, noviembre y diciembre de 2021, LinkedIn representaba sólo el 8% de todas las vulnerabilidades analizadas. Ahora, la red social profesional logró desbancar a DHL, que con el 14% del total de intentos de este trimestre, pasó a ocupar el segundo lugar.

El crecimiento de LinkedIn se enmarca en un aumento de las redes sociales como medio elegido por los ciberdelincuentes para los ataques de phishing. Éstas han comenzado a superar a las grandes compañías navieras y gigantes tecnológicos como Google, Apple o Microsoft. Es el caso de Whatsapp, que mantuvo su posición entre las 10 marcas más imitadas, con 1 de cada 20 de los ataques efectuados durante el primer trimestre del año.

En el caso específico de LinkedIn, la metodología más utilizada es contactarse con usuarios de esta red social a través de un correo electrónico que simula ser oficial, mediante el cual se los intenta atraer a que hagan clic en un enlace malicioso. Cuando esto sucede, se solicita nuevamente al usuario que inicie sesión a través de una versión falsa de LinkedIn, en el que se recopilará su información y credenciales.

Después de LinkedIn, el informe de Check Point Research señala que las plataformas de e-commerce (como DHL, FedEx, Maersk y AliExpress) fueron la segunda categoría más atacada, aprovechando el incremento general del comercio electrónico surgido de la pandemia.

¿Cómo funciona un ataque de phishing de marca? En estos casos, los delincuentes intentan imitar el sitio web oficial de una marca conocida, utilizando una dirección y un diseño de página web lo más parecido al original. El enlace a este sitio web falso se envía a personas específicas por correo electrónico, se puede redirigir a un usuario mientras está navegando o se puede activar desde una aplicación fraudulenta. El sitio web falso contiene por lo general un formulario destinado a robar

las claves de los usuarios, detalles de pago u otra información personal.

Según Omer Dembinsky, gerente del grupo de investigación de datos de Check Point Software, estos intentos de phishing son conocidos como “ataques de oportunidad”: se orquestan a gran escala, tratando de lograr que la mayor cantidad posible de personas compartan sin querer sus datos personales. Algunos de estos ataques buscan influenciar sobre las personas o robarles información, como sucede con LinkedIn, pero otros buscan instalar malware en redes y sistemas de empresas. El informe señala el caso de la empresa de transporte Maersk, que fue víctima este trimestre de ataques mediante correos electrónicos maliciosos que contenían documentos falsos del operador, lo que supuso un verdadero dolor de cabeza.

El informe de Check Point Research viene a confirmar algo que durante mucho tiempo se puso en duda: que las redes sociales un buen día se convertirían en uno de los sectores más atacados por grupos cibercriminales. Esas dudas se disiparon. Aunque Facebook dejó de estar entre los primeros diez puestos de phishing de marcas, LinkedIn ha pasado inesperadamente a ocupar su lugar. Los usuarios de esta red social, hoy más que nunca, deben capacitarse para no dejarse sorprender en los próximos meses.