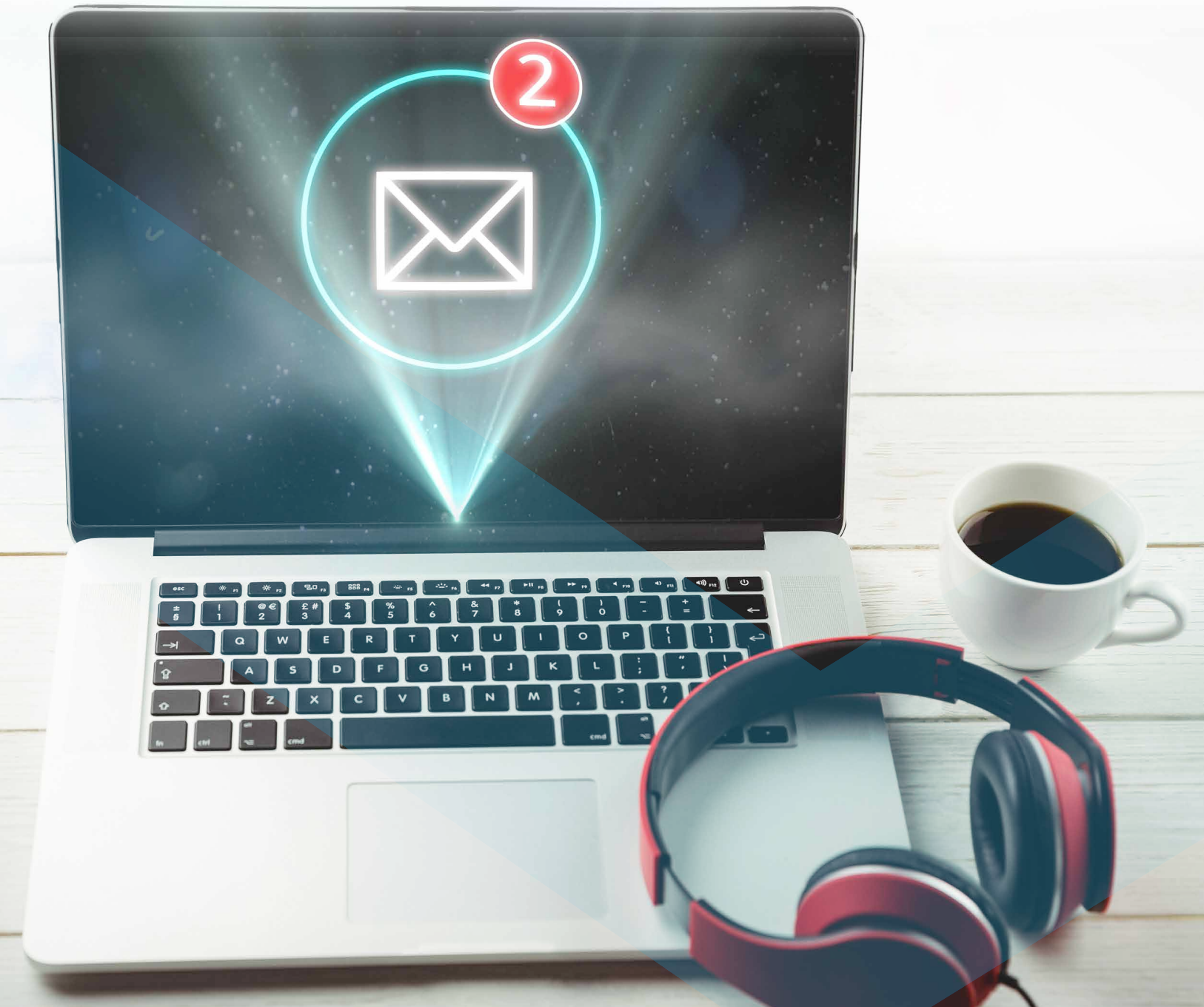
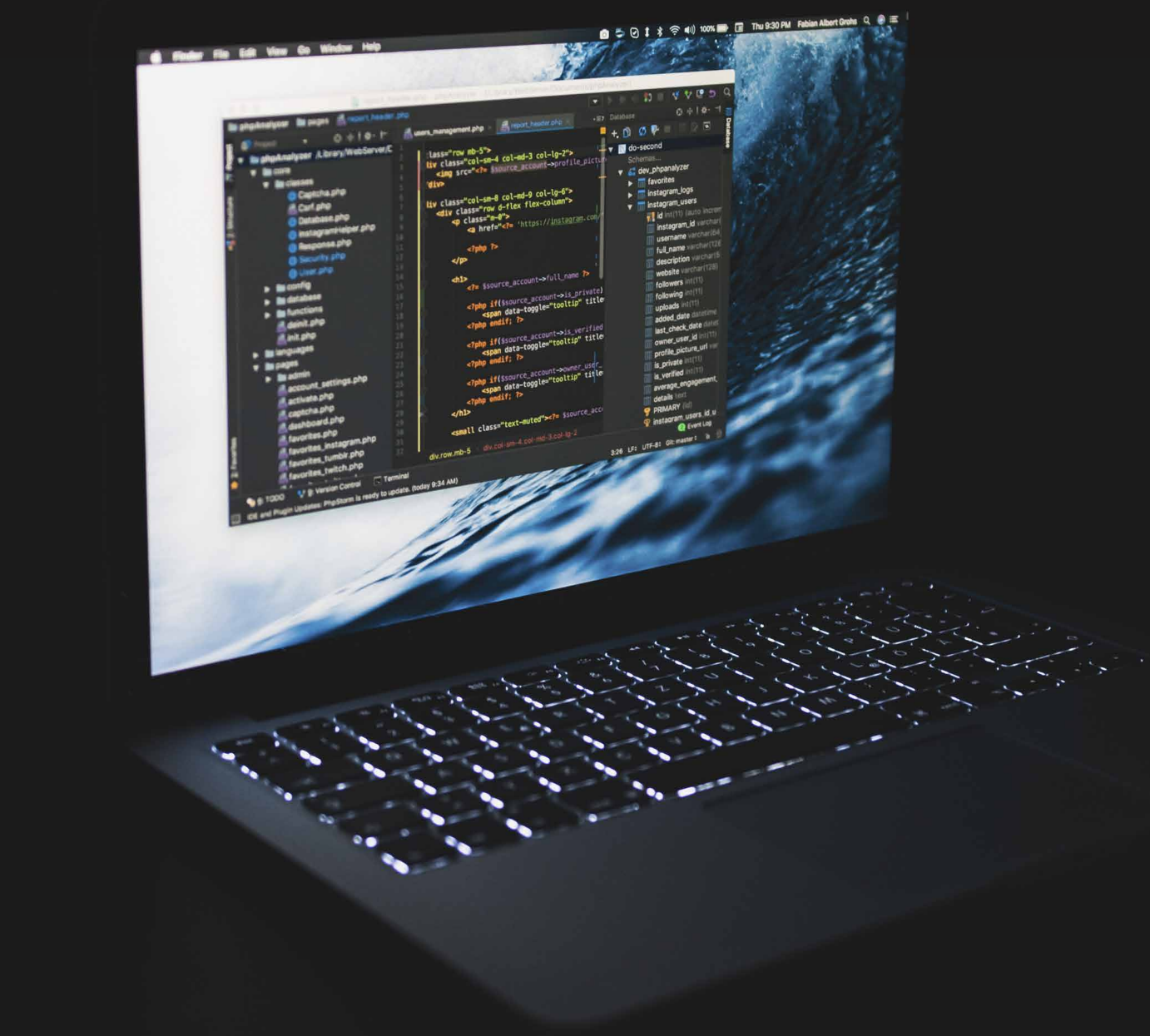
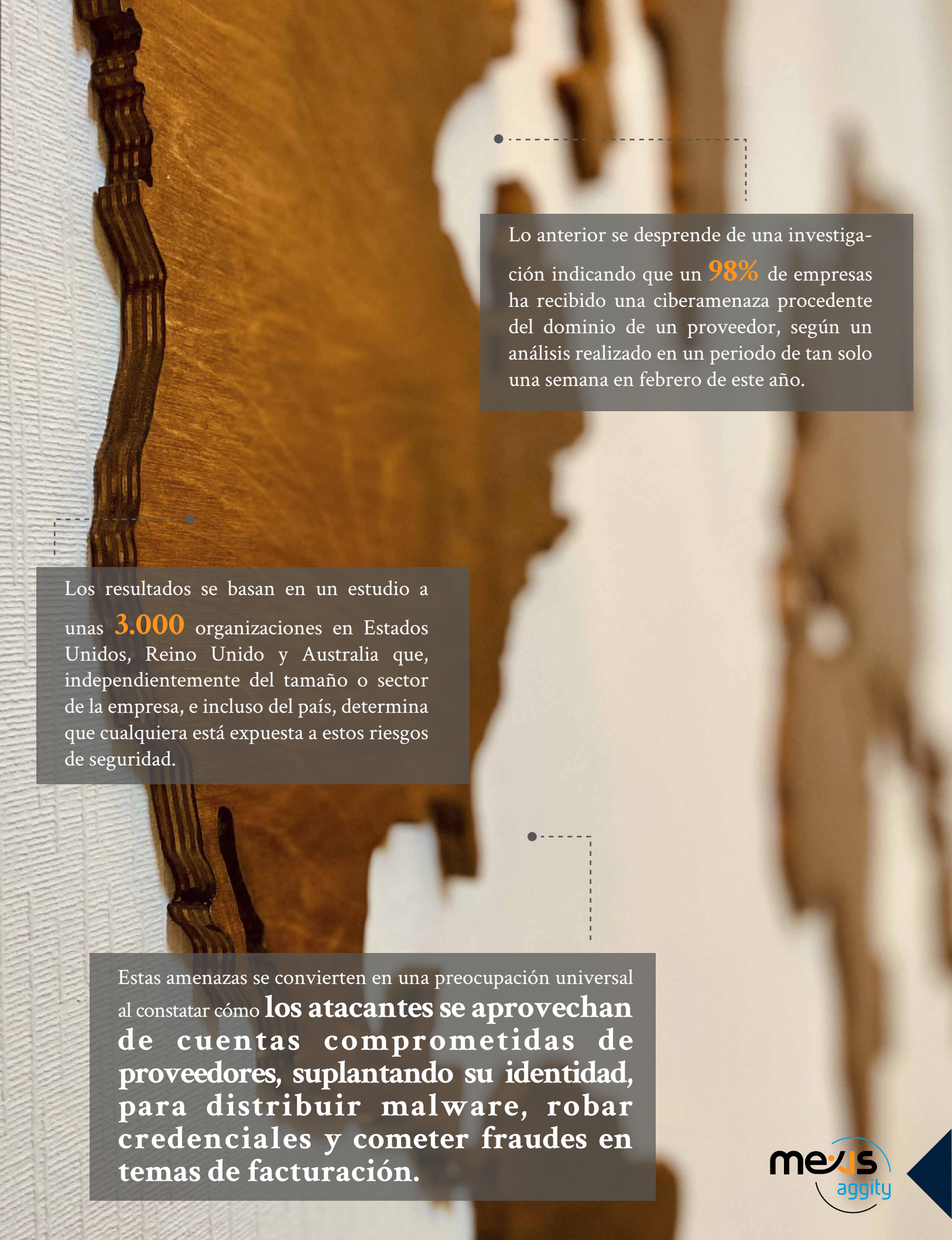
El 98% de las organizaciones ha recibido ataques por correo electrónico de supuestos proveedores



La cadena de suministro y el ecosistema de partners de las organizaciones se han convertido en un nuevo vector de ataque para los ciberdelincuentes.





Lo anterior se desprende de una investigación indicando que un **98%** de empresas ha recibido una ciberamenaza procedente del dominio de un proveedor, según un análisis realizado en un periodo de tan solo una semana en febrero de este año.

Los resultados se basan en un estudio a unas **3.000** organizaciones en Estados Unidos, Reino Unido y Australia que, independientemente del tamaño o sector de la empresa, e incluso del país, determina que cualquiera está expuesta a estos riesgos de seguridad.

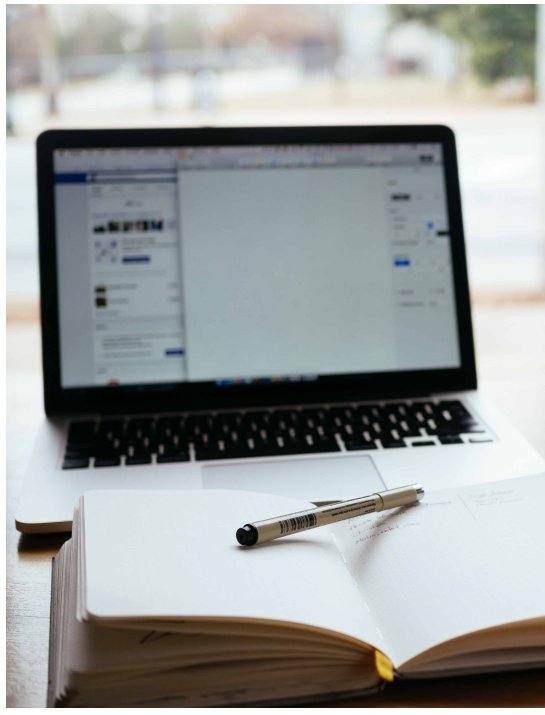
Estas amenazas se convierten en una preocupación universal al constatar cómo **los atacantes se aprovechan de cuentas comprometidas de proveedores, suplantando su identidad, para distribuir malware, robar credenciales y cometer fraudes en temas de facturación.**

Esta investigación se revela que las amenazas de proveedores suplantados y comprometidos son más propensas a emplear la ingeniería social para aprovecharse de la naturaleza humana, ya que el 74% de las amenazas es de tipo phishing o de impostor como los ataques de compromiso de correo electrónico corporativo. Menos del 30% de las amenazas enviadas desde dominios de proveedores estaba relacionada con malware.

Esto es a su vez una prueba más de que los atacantes se dirigen principalmente a las personas en lugar de atacar vulnerabilidades en la infraestructura de una organización. Los ciberdelincuentes están asimismo detrás de proveedores cloud explotando plataformas de colaboración populares, como Microsoft 365, Google G-Suite y Dropbox, para alojar o enviar más amenazas a un ritmo vertiginoso.

Respecto a este mismo estudio, tampoco es de extrañar que amenazas como la suplantación o spoofing de dominios solo representen el 3% del total de ataques enviados por parte de supuestos proveedores. A diferencia de otras amenazas mucho más extendidas, estas se suelen dirigir en concreto a muy pocas personas dentro de una organización.

Aunque ninguna compañía es inmune a las amenazas en las que se utilizan dominios de proveedores, las grandes organizaciones suelen estar más expuestas y experimentan más ataques de este tipo, cuadruplicando el número de mensajes fraudulentos recibidos que un cliente medio, según el análisis. Entre las organizaciones que sufren en mayor medida estas amenazas de supuestos proveedores están aquellas relacionadas con servicios financieros, fabricación, servicios públicos, comunicaciones, transporte, comercio mayorista y construcción.



No obstante, lo que sí funciona para que las organizaciones puedan defenderse de estos ataques es contar con una solución multicapa y holística de ciberseguridad. Una de las soluciones comprende la importancia de capacitar a los usuarios finales para que detecten y denuncien cualquier correo electrónico sospechoso a través de planes de concientización.

Automatizar la investigación y la respuesta a estos incidentes, con mayor visibilidad de qué proveedores suponen un riesgo, son otros de los avances al alcance hoy en día de todo tipo de organizaciones a través de herramientas de seguridad.

Fuente de información:
diarioti.com