[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en CDMX el 17/10/2022

# [Hillstone advierte que ransomware y malware derivados de un ciberataque son solo la punta del iceberg](http://www.notasdeprensa.es)

## Todas las empresas y organizaciones que han sufrido un ataque saben que si no se resuelve el problema de fondo pueden ser víctimas nuevamente de los hackers

En las últimas semanas se ha visto cómo diferentes organizaciones públicas y privadas han sido víctimas de los ciberdelincuentes, hechos que se destacan no solo por el impacto que tienen en las instituciones sino porque dejan al descubierto que el objetivo puede ser cualquiera. Al respecto, Hillstone Networks, proveedor líder de soluciones de seguridad de red y gestión de riesgos, explicó que el robo de información, ransomware, cryptomining o cualquier otro tipo de problema derivado de un ciberataque, solo es la punta del iceberg y que si las organizaciones no detectan cómo se perpetró tienen una gran posibilidad de volver a ser atacados. "Regularmente un ataque inicia cuando alguien dentro de la organización descargó un archivo malicioso, posteriormente el malware tiene varias opciones, escanear los dispositivos cercanos para evaluar si se puede propagar la infección, instalar nuevos programas en computadoras y servidores, moverse lateralmente para identificar dónde se guarda la información crítica, etc. Al final, lo único que se identifica es el resultado del ataque, que puede ser secuestro de información (ransomware), exfiltración de datos, robo de información confidencial, entre muchos otros", comentó Manuel Acosta, Director General para México en Hillstone Networks. Ante una crisis de este tipo, las organizaciones se dedican a levantar los servicios, reconstruir servidores, es decir, tratan de continuar la operación lo más pronto posible haciendo uso de respaldos y muchas veces empezando de cero. Sin embargo, solo se están enfocando en paliar el problema, no lo están resolviendo. "Todas las empresas y organizaciones que han sufrido un ataque saben que si no se resuelve el problema de fondo pueden ser víctimas nuevamente", reiteró Acosta. Ante esta situación, lo más recomendable es iniciar una "caza de amenazas" o threat hunting, para identificar ciertos indicadores de comportamiento (rastros) que hayan sido dejados durante la orquestación del ataque. De esta manera, ahora sí la organización sabe qué brechas debe cubrir para evitar una nueva crisis. Para ayudar a las organizaciones, Hillstone Networks ha incorporado el concepto de ciberresiliencia, que utiliza soluciones de visibilidad de amenazas y análisis de comportamiento para detectar amenazas avanzadas y mapearlas antes de que exploten, o bien, ayudar a las organizaciones que fueron víctimas de un ciberataque a aislar las vulnerabilidades y eliminar el problema desde su origen.

**Datos de contacto:**

Carlos Soto

Comunicación en Movimiento

+525532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/ransomware-y-malware-derivado-de-un](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Ciberseguridad

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)