NEWSLETTER

totalsec
Expertos en Ciberseguridad

No. 303 | Dic 20 - Dic 24

EL ATAQUE RANSOMWARE A KRONOS PODRÍA AFECTAR A SOLUCIONES BASADAS EN LA NUBE

DICIEMBRE 21, 2021/FUENTE: CIBER SECURITY NEWS[1]

Si hay una palabra que define a la perfección este 2021 esa es «RANSOMWARE«. El año que se despide ha estado marcado por un brutal incremento de estos ataques por parte de diversos grupos cibercriminales. Por desgracia, no vamos a despedir el año libres de este mal endémico. En Diciembre hemos visto varios casos, siendo uno de ellos el experimentado por Kronos Group, empresa proveedora de soluciones. El pasado 11 de diciembre, la empresa se vio afectada por un ataque ransomware que, o mucho cambia la cosa, o sus efectos no van a ser precisamente leves. Kronos es una compañía que ofrece soluciones basadas en la nube para administrar: tiempo, nómina, beneficios de empleados, análisis y otros. Estas soluciones son usadas por muchas empresas, las cuales podrían verse afectada por un parón en el servicio. El ataque ransomware a Kronos podría afectar a soluciones cloud.

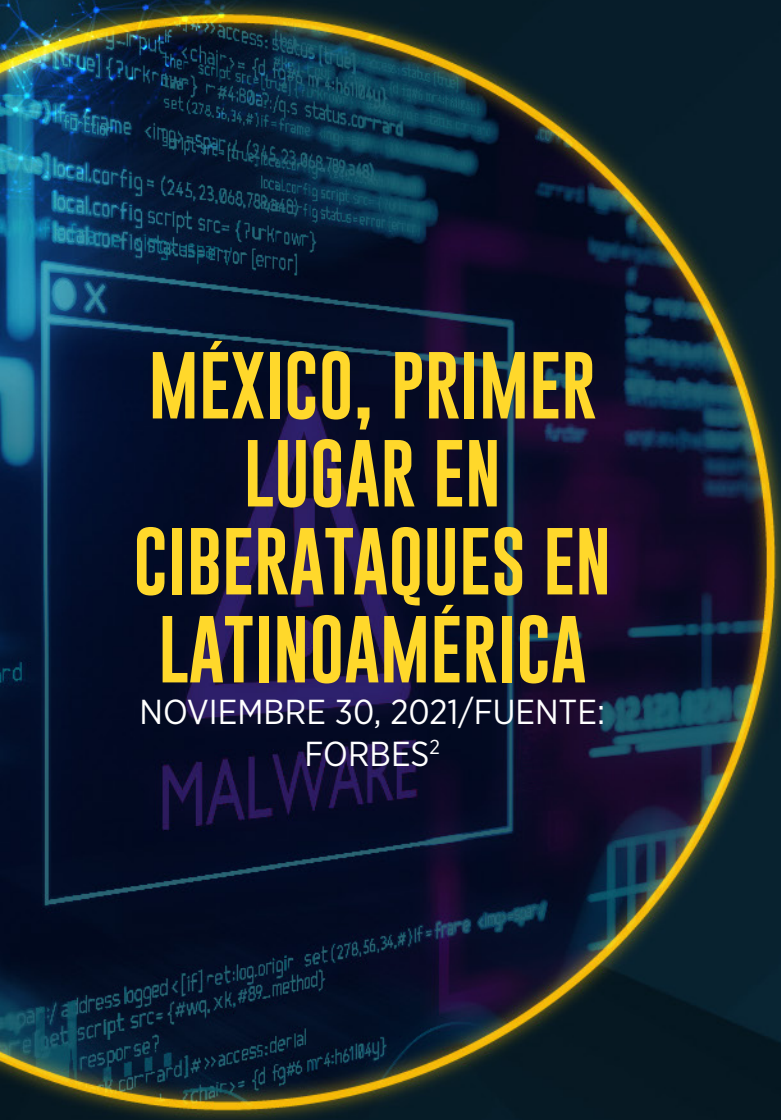
Kronos ha revelado recientemente que las soluciones UKG (resultado de su fusión con Ultimate Software) que utilizan «Kronos Private Cloud» no se están disponibles. Esta situación está afectando a empresas de sectores tan variados como: automoción, educación, gobiernos locales y más. entre las empresas/organismos más destacables que lo usan se encuentran Tesla, Community Bank o Temple University. La empresa ha emitido un comunicado, firmado por Bob Hughes, vicepresidente ejecutivo de UKG, en el que comenta: -«Como informamos anteriormente, a última hora del 11 de diciembre de 2021, nos percatamos de una actividad inusual que afectaba a las soluciones de UKG Kronos Private Cloud. Tomamos medidas inmediatas para investigar y mitigar el problema, y determinamos que se trataba de un incidente ransomware que afectaba a Kronos Private Cloud, la parte de nuestro negocio donde se implementan UKG Workforce Central, UKG TeleStaff, extensiones de atención médica y soluciones de programación bancaria»-.

Las defensas de Kronos no funcionaron

El servicio que ofrece la empresa no está exento de defensas; cuenta con firewalls, autenticación multifactor y transferencias cifradas para evitar el acceso no autorizado a sus sistemas. A pesar de ello, los ciberdelincuentes lograron vulnerar la seguridad de los sistemas; los efectos se desconocen, pero podríamos estar hablando de cifrado de los servidores. Debido a ello, desde Kronos han querido anunciar que sus soluciones KPC no están disponibles; cabe la posibilidad que pasen varias semanas antes de que los sistemas vuelvan a estar operativos. Durante este pedido, la empresa está recomendando a sus clientes «evaluar e implementar protocolos alternativos de continuidad comercial relacionados con las soluciones UKG afectadas«-. Este ciberataque se ha dado en un periodo muy complicado, pues la navidad llama a la puerta: vacaciones, pagos de bonos, reducción temporal de la plantilla de trabajo... El ataque ransomware a Kronos podría afectar a soluciones cloud.

> El ataque ransomware a Kronos podría afectar a soluciones basadas en la nube y durar varias semanas hasta ponerle solución

[1]Fuente: https://cybersecuritynews.es/el-ataque-ransomware-a-kronos-podria-afectar-a-soluciones-basadas-en-la-nube/



MÉXICO, PRIMER LUGAR EN CIBERATAQUES EN LATINOAMÉRICA

NOVIEMBRE 30, 2021/FUENTE: FORBES[2]

Este 30 de noviembre es el Día Internacional de la Seguridad Informática, por lo que expertos alertaron sobre el incremento de ataques cibernéticos y robo de información tanto en empresas como en el sector público, donde México es un blanco importante, de acuerdo con datos de la multinacional Fortinet.

Tan solo durante el primer semestre del año, dijeron, se registraron más de 91,000 millones de intentos de ciberataques en Latinoamérica, de los cuales más de 60,000 millones ocurrieron en México durante el primer semestre de 2021, lo que ubica al país en el primer lugar de la región frente a este tipo de amenazas. México ocupó el primer lugar de la región con 67% de intentos de ataque, seguido por Brasil con 17.8% y Perú con 5.1%, según Fortinet.

"Cada vez es más común escuchar en las noticias acerca de ataques ransomware, en los que las empresas son víctimas del intento o robo de información para después exigirles una recompensa a cambio de la misma. Esta es una práctica que no es nueva y que, desafortunadamente, ha aumentado a medida que crece la digitalización", señaló Martín Malievac, director de Investigación y Desarrollo de Napse, empresa especializada en soluciones tecnológicas para el retail, citado en el comunicado.

"Una vez que te secuestran el servidor o tu información -incluida la de socios y clientes-, solo tienes dos opciones: accedes al chantaje o reinstalas todo desde cero. Ambas opciones implican desembolsar grandes cantidades de dinero, sin mencionar el tiempo y recurso humano que debes invertir para corregir el problema", agregó.

México ocupó el primer lugar de la región con 67% de intentos de ataque

La ciberseguridad, agregó, se ha convertido en un tema crítico para todo tipo de organizaciones, sin importar su tamaño, ya que la vulnerabilidad en los sistemas puede causar estragos económicos y reputacionales en cualquier compañía.

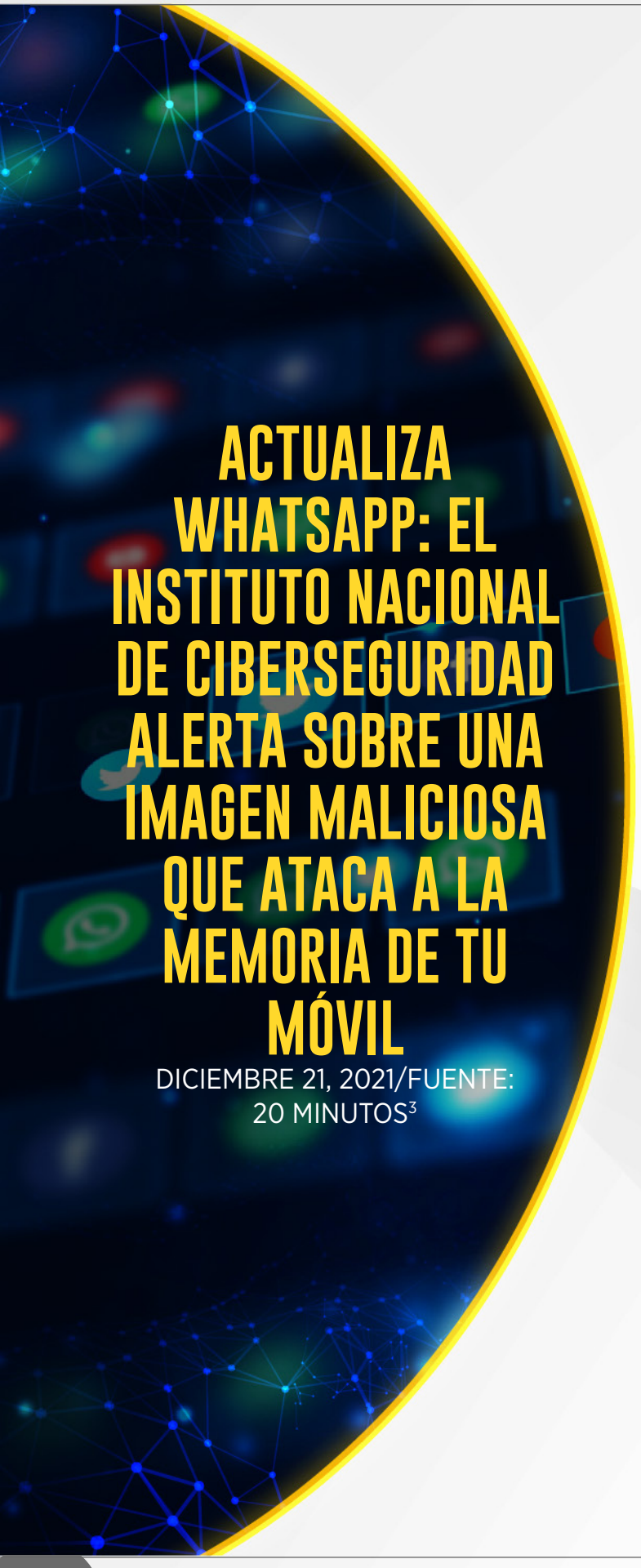
Justo a principios de junio se dio a conocer que Lotería Nacional había sufrido un ciberataque y que información de la dependencia fue sustraída por cibercriminales. "En torno al ataque cibernético, a los sistemas de la Lotería Nacional, se informa que hace dos semanas se detectó una sustracción de información en el área administrativa de Lotería Nacional, antes Pronósticos, por parte de delincuentes que operan a nivel internacional", informó la institución en su momento. Lotenal agregó entonces que inició la gestión de un programa de modernización de los sistemas informáticos y que contaba con respaldo de la información en todas las áreas, además de que los concursos y sorteos operan con normalidad.

Para evitar que esto ocurra, el especialista recomendó realizar con regularidad pruebas de penetración, las cuales están diseñadas específicamente para encontrar vulnerabilidades o "agujeros" que los atacantes aprovechan para ingresar a los sistemas. Este tipo de software, además de identificar debilidades, las soluciona y alerta de forma rápida.

Tomando en cuenta que cada vez más empresas laboran bajo un esquema híbrido, entre la oficina y los hogares, la infraestructura en la nube es la mejor aliada para la protección de la información, en lugar de instalar un servidor, con el riesgo de que alguien externo o interno acceda a él, robe la data o lo deje inhabilitado. "La nube es una buena herramienta porque es una forma de tomar una solución que está en internet, pero nos da herramientas para generar mayor seguridad como alertas y acceso con técnicas como el tóken, generar usuarios con determinados tipos de permisos, entre otras funcionalidades", añadió. Con el crecimiento del comercio electrónico, las empresas no son las únicas expuestas a un ciberataque, por lo que las medidas de protección deben extenderse a sus usuarios, agregó el especialista.

Considerando los costos y pérdidas que implica un ataque cibernético, resulta indispensable invertir en personal experto y plataformas seguras o contar con aliados para que las compañías reduzcan los peligros y no vean comprometida su operación.

[2]Fuente: https://www.forbes.com.mx/negocios-mexico-primer-lugar-en-ciberataques-en-latinoamerica/



ACTUALIZA WHATSAPP: EL INSTITUTO NACIONAL DE CIBERSEGURIDAD ALERTA SOBRE UNA IMAGEN MALICIOSA QUE ATACA A LA MEMORIA DE TU MÓVIL

DICIEMBRE 21, 2021/FUENTE: 20 MINUTOS[3]

Sin duda, la aplicación más popular de mensajería instantánea es WhatsApp, no obstante, también es la principal app que emplean los ciberdelincuentes para introducir malware en los dispositivos de los usuarios.

En el caso de que no tengas actualizado WhatsApp o WhatsApp Business con su última versión, debes saber que tu dispositivo puede estar expuesto a un nuevo ataque que podría infectar tu móvil con tan solo recibir una imagen maliciosa.

El Instituto Nacional de Ciberseguridad (INCIBE) ha informado en un comunicado que los usuarios con la versión 2.21.22.6 o anteriores están expuestos a dicho fallo de seguridad en Android. Esta acción maliciosa consiste en recibir una imagen que puede provocar alteraciones en la memoria del dispositivo.

Los usuarios que tengan la versión 2.21.22.6 de WhatsApp en Android (o anteriores) están expuestos a un fallo de seguridad. El ataque se produce a través de un "imagen maliciosa" que corrompe la memoria del dispositivo.

Para evitar esta situación, los usuarios deben actualizar la última versión de WhatsApp en Android con el fin de evitarlo, asimismo, el ataque puede llevarse a cabo a través de la red y no requiere ningún tipo de autentificación.

INCIBE afirma que el componente vulnerable es Image Blurring Handler, teniendo en cuenta que los ciberdelincuentes pueden crear y enviar una imagen maliciosa que puede provocar escritura fuere de límites del búfer o corrupción de la memoria del dispositivo por falta de comprobación del código de desenfoque cuando se recibe.

Las consecuencias de este ataque son poner en riesgo la confidencialidad e integridad de los datos y programas instalados. INCIBE recuerda en su web la importancia de mantener los sistemas y aplicaciones siempre actualizados.

[3]Fuente: https://www.20minutos.es/tecnologia/ciberseguridad/actualiza-whatsapp-el-instituto-nacional-de-ciberseguridad-alerta-sobre-una-imagen-maliciosa-que-ataca-a-la-memoria-de-tu-movil-4930608/?autoref=true

NEWSLETTER

totalsec
Expertos en Ciberseguridad