BOLETÍN INFORMATIVO

INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 29 de abril de 2022.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la trasformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanos y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

Detectada una nueva campaña con *malware* Emotet

Esta semana, INCIBE ha detectado un repunte del *malware* Emotet, un tipo de troyano que se propaga a través del envío de correos fraudulentos. El objetivo es que el receptor abra los archivos adjuntos del email y descargue e instale un adjunto malicioso. Otra opción que buscan los ciberdelincuentes es que acceda a un enlace no confiable donde descargar el *malware*, para finalmente pasar a formar parte de la *botnet* Emotet.

Cualquier empleado o empresario que haya descargado y ejecutado el archivo, debe realizar un escaneo de todo el equipo con el antivirus y seguir las instrucciones marcadas por el mismo para eliminar el *malware*. También es recomendable que desconecte dicho equipo de la red principal de la empresa para evitar que otros dispositivos puedan verse infectados.

Más información en: https://www.incibe.es/protege-tu-empresa/avisos-seguridad.

Ataque de *ransomware*, ¿cómo puedo recuperar la información?

El *ransomware* es un tipo de *malware* que se introduce en los equipos y dispositivos móviles conectados a Internet, impidiendo el acceso a la información, generalmente cifrándola, y solicitando un rescate para que vuelva a ser accesible o no sea divulgada. El *malware* intenta propagarse al resto de los sistemas conectados a la Red, poniendo así en riesgo la continuidad de negocio.

¿Qué pasos debe seguir un empresario que se vea afectado por esta amenaza? En este artículo de INCIBE se recomienda crear una imagen de respaldo de las unidades cifradas antes de proceder con las instrucciones de eliminación del *ransomware*. Cabe destacar que es importante no saltarse ningún paso de los enumerados en el post y realizarlos en el orden correcto.

Más información en: https://www.incibe.es/protege-tu-empresa/blog.

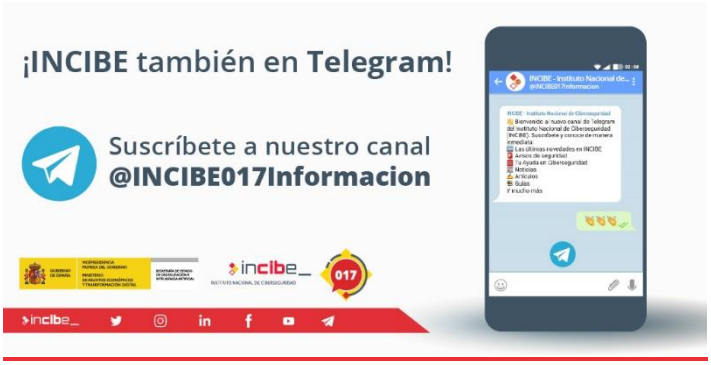
comunicacion@incibe.es
@incibe
017 TU AYUDA EN CIBERSEGURIDAD
www.incibe.es
Av. José Aguado 41 / 24005 León
T. (+34) 987 877 184

Cómo actuar en caso de un ataque de ransomware

Por otro lado, en esta nueva sección web, INCIBE se centra en la repercusión que tendría para un usuario básico verse afectado por una amenaza tipo *ransomware*. Por eso, explica, paso por paso, cómo actuar si se ha sufrido un ataque de este tipo. Los principales son: iniciar el equipo Windows en modo seguro con funciones de red, eliminar el *ransomware* con una herramienta de tipo cleaner, realizar un segundo análisis para confirmar que el equipo está limpio y restaurar los archivos cifrados por el *ransomware*.

Antes de comenzar con los siguientes pasos, desde INCIBE se recomienda hacer una copia de la información almacenada en el disco, aunque esté cifrada, ya que el proceso que se describe en este artículo podría suponer la eliminación de archivos, provocando que no se puedan recuperar de ninguna forma.

Más información en: https://www.osi.es/es/como-actuar-en-caso-de-un-ataque-de-ransomware.



Suscríbete al nuevo canal de Telegram de INCIBE

Para más información:

https://www.incibe.es/
https://www.incibe.es/protege-tu-empresa
https://www.osi.es/es
https://www.is4k.es/
https://www.incibe-cert.es/

Redes sociales:

FB IG TW YT LI