CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR

ARCOTEL

CIBERCONSEJOS "PROTÉGETE DEL RANSOMWARE"

https://www.ecucert.gob.ec/

@EcuCERT_EC

TABLA DE CONTENIDOS

Definición

Ransomware es un malware diseñado para cifrar archivos en un dispositivo.

Una particularidad es que los actores malintencionados exigen un rescate a cambio del descifrado. *ransom (rescate)* *ware (producto o mercancía).*

En los últimos años, los incidentes de ransomware se han vuelto cada vez más frecuentes entre las entidades gubernamentales estatales, locales.

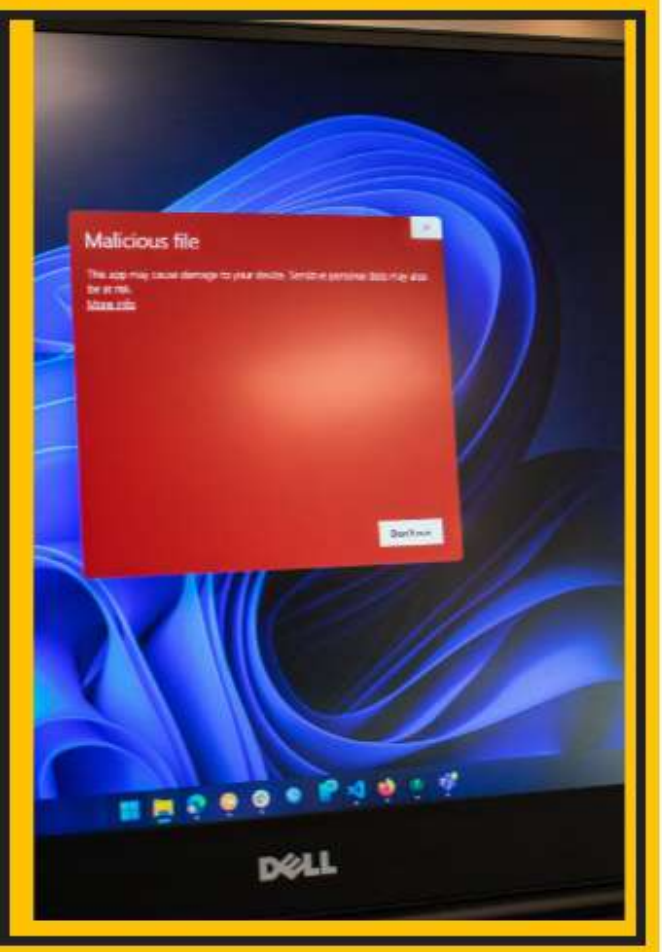

Ilustración asociada a Ransomware

TIPOS DE RANSOMWARE

Hoax ransomware

- También conocido como ransomware simulado.
- Los atacantes simulan el cifrado del dispositivo y emplean técnicas de ingeniería social para extorsionar al usuario, exigiéndole un pago por recuperar sus archivos o evitar que sean eliminados.

Scareware

- Emplea un anuncio sobre una supuesta infección en el equipo e indican que se debe dar clic en un enlace para descargar un programa de limpieza; siendo en este caso, el malware.

Bloqueadores de pantalla

- Los ciberdelincuentes impiden el acceso al dispositivo a través de una ventana que ocupa toda la pantalla; en esta ventana pueden mencionar que los archivos se encuentran cifrados y el procedimiento para recuperar la información.

TIPOS DE RANSOMWARE

1. Hoax ransomware
2. Scareware
3. Bloqueadores de pantalla
4. Ransomware de cifrado:
5. Doxware

Ransomware de cifrado

- Su principal objetivo es el cifrado de la información.
- Se considera el tipo de ransomware más peligroso ya que emplea técnicas de cifrado avanzadas evitando que los datos puedan ser descifrados.

Doxware

- Adicional al cifrado de la información, se presentan amenazas con la divulgación de información

FORMAS DE INFECCIÓN

Los ciberdelincuentes emplean diferentes maneras para infectar a la víctima:

Aprovechar vulnerabilidades existentes en los sistemas operativos, aplicaciones o software de los equipos.

Hacer uso de ingeniería social para que instalen el malware; emplear correos electrónicos falsos con supuestas actualizaciones de software.

Dirigir a las víctimas a sitios web infectados a fin de que descarguen el malware; aprovechando las vulnerabilidades existentes en el navegador.

MEDIDAS DE PROTECCIÓN

En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR el rescate.

Realizar periódicamente copias de respaldo de la información crítica.

No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.

Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.

Mantener actualizados, y bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.

MEDIDAS DE PROTECCIÓN

Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.

En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de des encriptado en el caso de existir) / https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)

Implementar un plan de respuesta a emergencias de la Organización/Institución.

En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.