BOLETÍN ESPECIAL DE SEGURIDAD INFORMÁTICA N.- 2019-ESFORSE-TICS-002, SOBRE MEDIDAS DE PREVENCIÓN ANTE EL MALWARE RANSOMWARE.

¿Qué es el malware RANSOMWARE?

El ransomware es un software malicioso empleado por los cibercriminales para secuestrar tu equipo o ciertos archivos que almacena, y luego pedirte el pago de un rescate a cambio de su recuperación.

ALCANCE

Son muchas las formas en que puede ingresar a una computadora, pero como suele ocurrir, las técnicas terminan siendo tácticas de **Ingeniería Social** o el uso de vulnerabilidades de software para instalarse silenciosamente en la máquina de la víctima.

MEDIDAS PARA PREVENIR EL MALWARE RANSONWARE:

- **Mantener copias de seguridad periódicas (backups) de todos los datos importante**s. Es necesario mantener dichas copias aisladas y sin conectividad con otros sistemas, evitando así el acceso desde equipos infectados.
- **No utilizar cuentas con privilegios de administrador,** reduciendo el potencial impacto de la acción de un ransomware.
- **Permanecer atentos ante intentos de aplicación de ingeniería social para extraer información PHISHING** (utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.)
- **Desconéctate del Wi-Fi o quita el cable de red de inmediato**. Si ejecutaste un archivo que sospechas que puede tratarse de un ransomware, pero aún no apareció la pantalla característica en tu computadora, si actúas muy rápido, quizá puedas detener la comunicación con el servidor C&C antes de que termine de cifrar tus archivos.
- Usa el antivirus **BITDEFENDER**. No desactives la detección mediante heurísticas ya que esto ayuda a capturar muestras de ransomware que aún no hayan sido detectadas formalmente.
- **Activa la opción de mostrar las extensiones** de los archivos en el menú de configuración de Windows. Esto hará mucho más fácil detectar archivos potencialmente maliciosos. Mantenerse alejado de extensiones como '.exe', '.vbs' y '.scr'. Los estafadores pueden usar varias extensiones para camuflar un fichero malicioso como un video, una foto o un documento (como chicas-calientes.avi.exe o doc.scr).

REPORTE DE INCIDENTES:

Reporte el incidente al Departamento de TICS, a través de red telefónica interna mediante la ext. 194