¿Qué es ransomware?

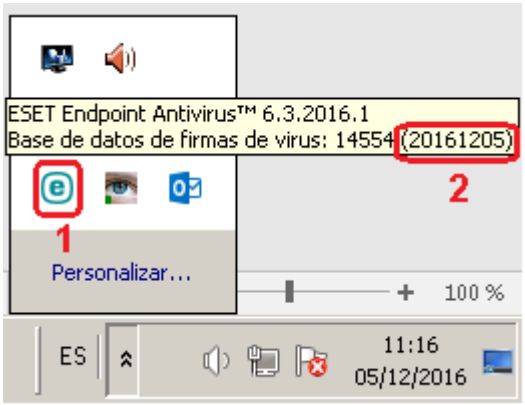
El ransomware es un software malicioso empleado por los cibercriminales para secuestrar su equipo o ciertos archivos que almacena, y luego pedirle el pago de un rescate a cambio de su recuperación. Lamentablemente, el ransomware es un medio cada vez más popular mediante el cual los creadores de malware extorsionan a empresas y consumidores por igual.

¿Qué se puede hacer al respecto?

- Verificar que la base de firmas del antivirus se encuentre siempre actualizada a la fecha junto con todos sus módulos o componentes instalados y activados, en caso de presentar alguna anomalía con el sistema antivirus, comuníquese con el Departamento de Tecnologías de Ia Información.

  Para verificar el estado del Antivirus:

  1. Ubicar el cursor en el icono del antivirus.
  2. En la información mostrada, verificar que la fecha se encuentre al día(aaaammdd)



- Se recomienda fuertemente que se desinstalen de los equipos todo tipo de software sospechoso como por ejemplo toolbars, drivers, codecs, screensavers, gestores de descarga y juegos puesto que son puertas de ingreso de malware.
- Si desea instalar un software, no descargarse de sitios como por ejemplo “Softonic” ya que dichos instaladores son modificados para incluir malware. Siempre se deben obtener los instaladores desde el sitio oficial del software o solicítelo a TI.
- Es muy recomendable realizar copias de seguridad regulares para poder restaurar los archivos infectados y minimizar los daños, pudiendo realizarlos en unidades externas o en la nube.
- No abrir correos de remitentes extraños o sospechosos, manténgase alerta y piense dos veces antes de abrir adjuntos de correo o de hacer clic en archivos de fuentes desconocidas. Tenga cuidado con archivos sospechosos con extensiones ocultas como “.pdf.exe”