PROCEDIMIENTO PARA ELIMINACION DE MALWARE

VIRUS DE MSN

1. Descargar la herramienta Process Explorer de la dirección http://av.uan.mx/tools.
2. Ejecutar la herramienta e identificar el o los procesos siguientes: (jusched.exe, fotos.mx, hfjd.exe, msnl.exe, foto26.com) que se está ejecutando en la PC y detenerlos.
3. Activar las opciones de carpetas y búsquedas y cambiar la configuración para visualizar archivos ocultos, si la opción no está habilitada para modificar estas opciones tiene que descargar la herramienta de Widetool de la ruta http://av.uan.mx/tools y ejecutar el script.
4. Buscar los archivos de los procesos que se detuvieron en el paso 2 en toda la PC y eliminarlos, (si se encuentra en una carpeta eliminar la carpeta).
5. Eliminar archivos temporales de la computadora y de internet.
6. Entrar al registro buscar y eliminar las entradas que coincidan con los archivos eliminados.
7. Entrar a msconfig y deshabilitar el inicio de los procesos de los archivos eliminados y cualquier otro archivo raro.
8. Reiniciar la PC y volver a ejecutar la herramienta de Process Explorer para verificar que no se hayan ejecutado los procesos de los archivos eliminados.

VIRUS DE CORREO ELECTRONICO

1. Descargar la herramienta Process Explorer de la dirección http://av.uan.mx/tools.
2. Ejecutar la herramienta e identificar el o los procesos siguientes: (sym.cpl, syr.exe, syr2.exe).
3. Activar la opción de carpetas y búsquedas y cambiar la configuración para visualizar archivos ocultos, si la opción no esta habilitada para modificar estas opciones tiene que descargar la herramienta de Widetool de la ruta http://av.uan.mx/tools y ejecutar el script.
4. Buscar los archivos de los procesos que se detuvieron en el paso 2 en toda la PC y eliminarlos, si se encuentra una carpeta con el nombre CMOS, eliminar esta carpeta.
5. Eliminar archivos temporales de la computadora y de internet.
6. Entrar al registro y eliminar las entradas que coincidan con los archivos y cualquier otro archivo raro.
7. Entrar a msconfig y deshabilitar el inicio de los procesos de los archivos eliminados y cualquier otro archivo raro.
8. Reiniciar la PC y volver a ejecutar la herramienta de Process Explorer para verificar que no se hayan ejecutado los procesos de los archivos eliminados.

DESINFECTAR MEMORIA USB

1. Activar la opción de carpetas y búsquedas y cambiar la configuración para visualizar archivos ocultos, si la opción no está habilitada para modificar estas opciones tiene que descargar la herramienta de Widetool de la ruta http://av.uan.mx/tools y ejecutar el script.
2. Conectar la memoria USB y abrir de forma segura desde el Explorador de Windows.
3. Eliminar los archivos raros que aparezcan y de acceso directo de la memoria.
4. Para regresar los atributos de los archivos a su estado original siga los siguientes pasos:
    - iniciar la consola de Windows dando clic en inicio y ejecutar el comando **CMD**.
    - Entrar a la memoria por línea de comandos escribiendo en la consola **D: Enter**, según sea la unidad asignada.
    - Escribir el comando **attrib /d /s -r -h -s *.*** para regresar los atributos a todos los archivos de la memoria.
    - Cerrar la consola de Windows.

5. Verificar la información de la memoria USB y retirarla.