Guía de Seguridad

Fecha de publicación: 20/03/2020

Tema: Eliminación del malware **"Corona-Virus-Map.com"**

1. Introducción

El (COVID-19) es nuevo virus que forma parte de la familia de los coronavirus. El primer caso fue detectado el 31 de diciembre de 2019 en la ciudad china de Wuhan y desde entonces se ha expandido enormemente en todo el mundo, a pesar de las distintas medidas adoptadas por los países para frenar la pandemia. Debido a la preocupación por esta pandemia, muchas personas buscan información del estado actual de su país y cómo se compara con el resto del mundo. Los Ciberdelincuentes se aprovecharon de esta situación clonando la apariencia de un mapa legítimo de Coronavirus de la Universidad Johns Hopkins, y han lanzado un programa malicioso llamado **"Corona-Virus-Map.com"**, sin embargo este mapa está diseñado para causar infecciones en cadena, es decir descargar e instalar sigilosamente otros malwares, concretamente el AZORult, el cual busca comprometer la integridad del equipo y podría provocar graves problemas de privacidad, pérdidas de información financiera, perdida de dinero y/o robo de identidad.

Este mapa generalmente es distribuido, mediante archivos adjuntos de correo electrónico, anuncios maliciosos en línea, ingeniería social y vulnerabilidades en softwares.

2. Descripción

A continuación los pasos para la eliminación del malware, en caso de que su equipo haya sido infectado:

2.1. ¿Como verifico si estoy infectado?

Para descubrir si su equipo está infectado, debe verificar los procesos **"WindowsFormsApp2"** y **"Журналы и оповещения производительности.exe"** en el Administrador de tareas de Windows, en caso de que estos se encuentren en ejecución su equipo está infectado y debe seguir los pasos para la eliminación del virus.

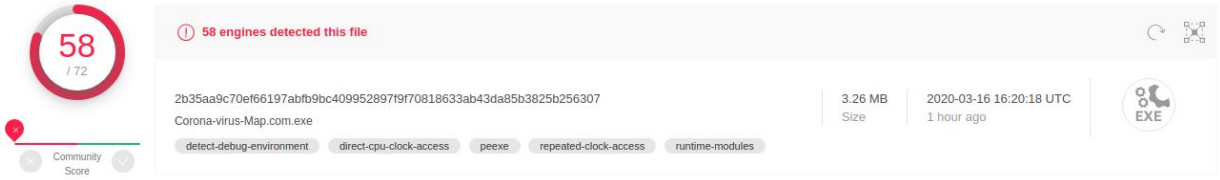
2.2. ¿Como eliminar el "Corona-Virus-Map.com"?

La eliminación se puede realizar de dos maneras:

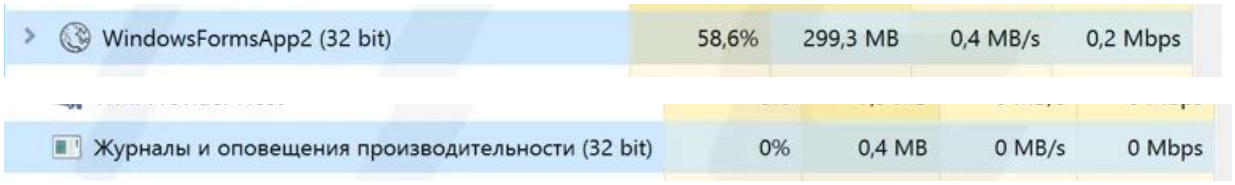
- **Automática:**

A través de una herramienta de detección y eliminación de malware y/o cualquier antivirus, debe seguir los siguientes pasos:

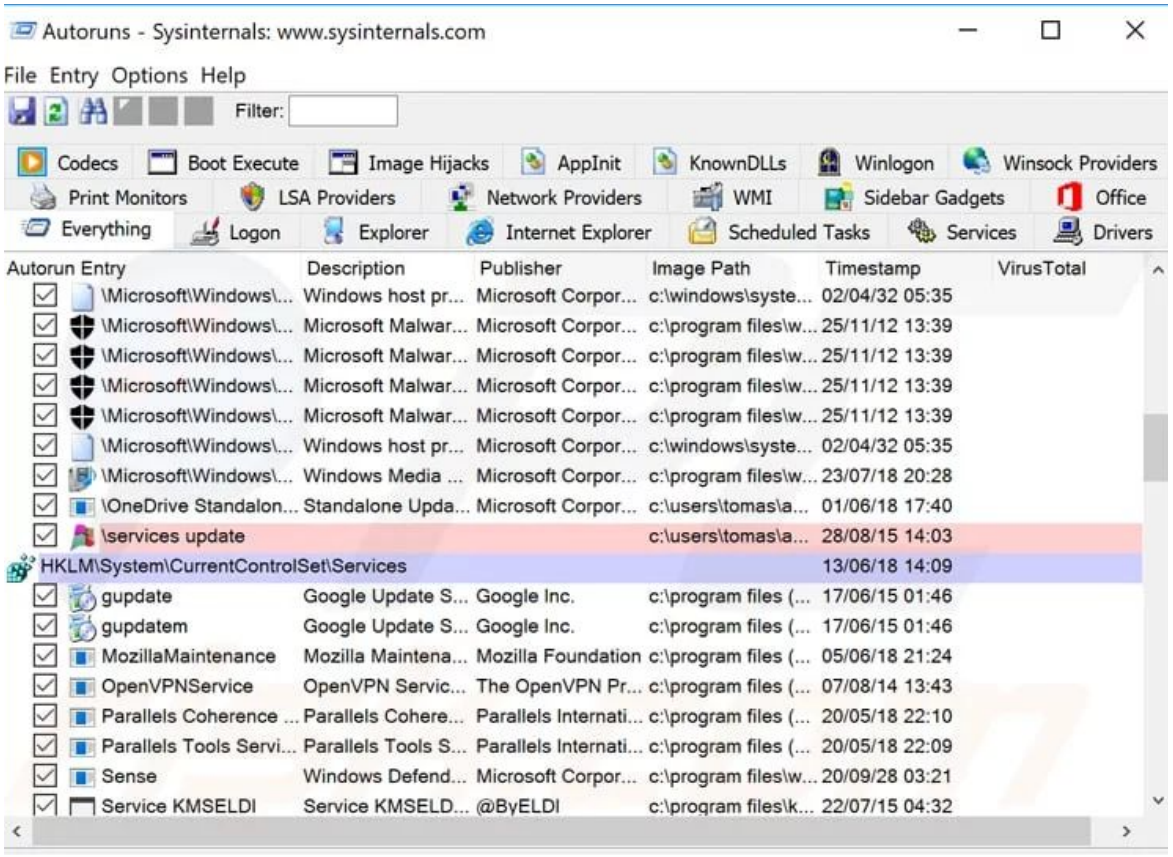
  - Actualizar la base de datos de su antivirus, ya que la mayoría de las herramientas han agregado recientemente a sus bases de datos este malware,
  - Realizar un escaneo al equipo infectado, con esto su herramienta procederá a la identificación y eliminación del malware.



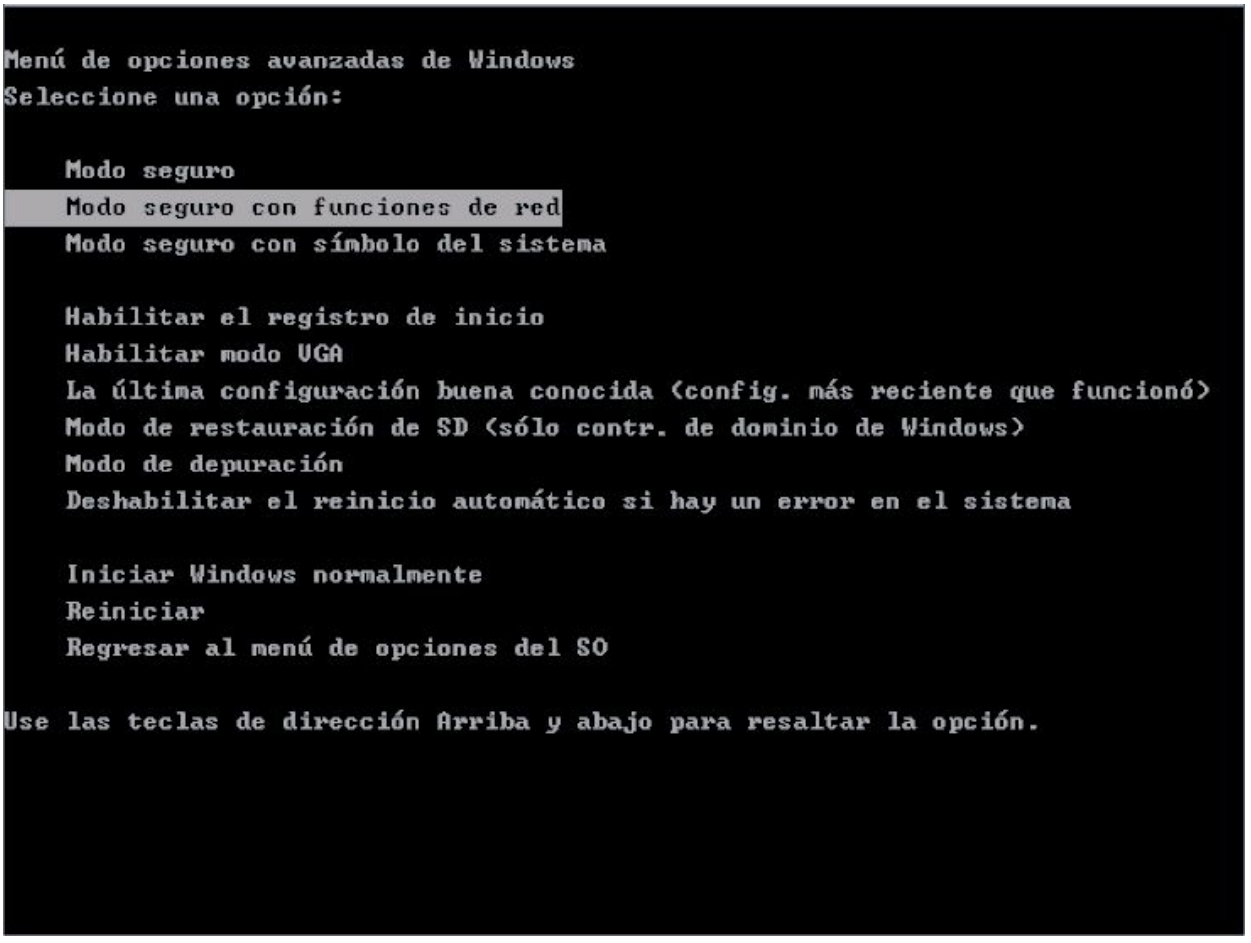
- **Manual:**
  - Identificar el proceso asociado al malware que desea eliminar, en este caso el **"WindowsFormsApp2"** y el **"Журналы и оповещения производительности.exe"**:



  - Descargar la herramienta de Microsoft llamada Autoruns (permite visualizar los programas que inician de manera automática, así como sus registros y las ubicaciones).



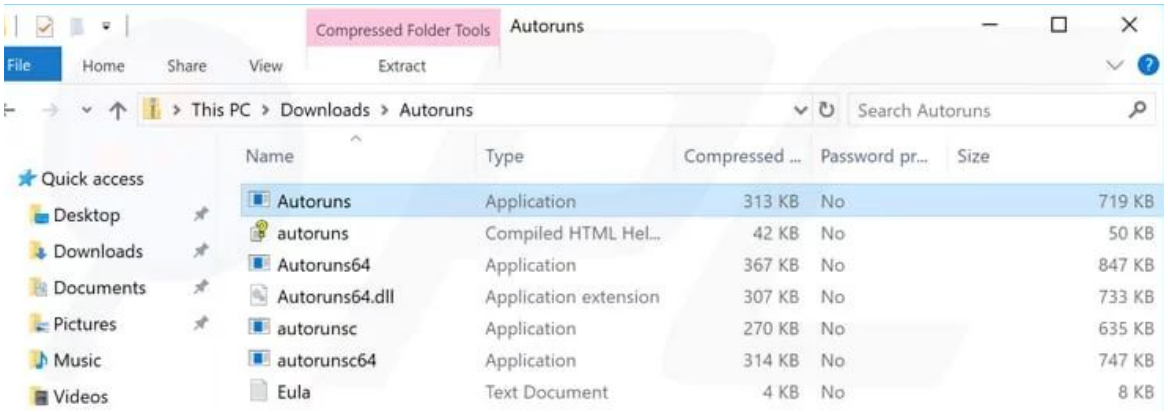
- Iniciar el equipo en modo seguro:
  - Para **usuarios de Windows XP y Windows 7:**
    - Haga clic en ***ñreiniciarò***, y durante el proceso de inicio de su equipo, presione la tecla ***ñF8ò*** en su teclado varias veces hasta que vea el menú ***ñOpciones avanzadas de Windowsò*** y,
    - Seleccione ***ñModo seguro con funciones de redò***.



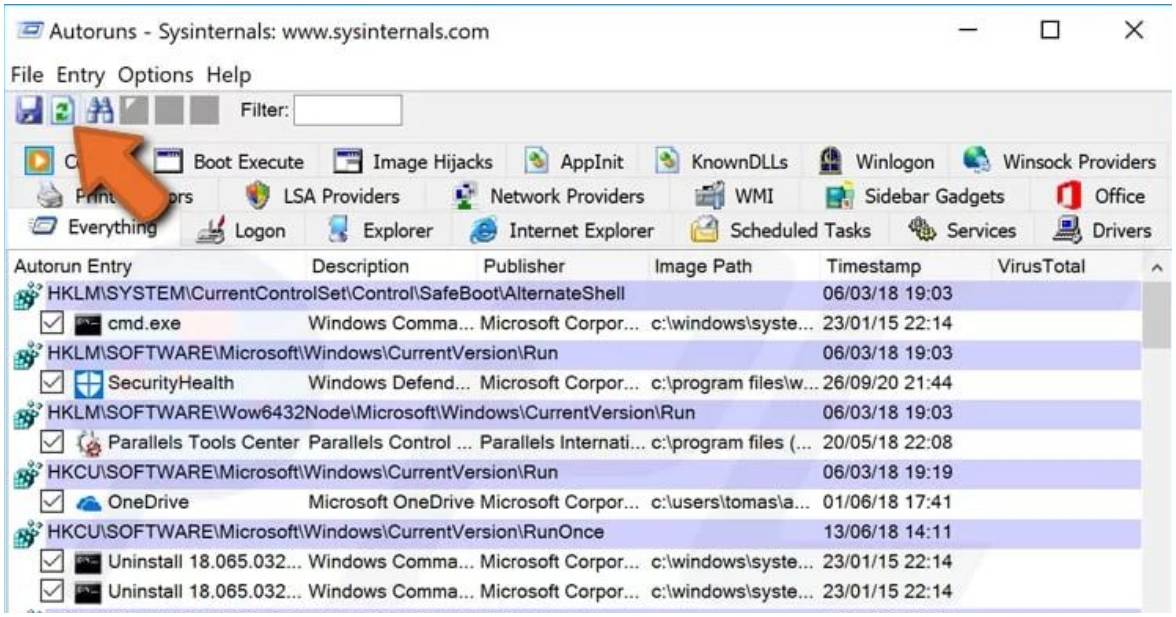
- Para **usuarios de Windows 8:**
  - Presione el botón de ***ñWindows ( )+ Cò***,
  - Haga clic en ***ñConfiguraci· nò > ñCambiar configuraci· n de PCò > ñActualizar y recuperarò > ñRecuperarò***,
  - En esta ventana presione el botón de ***ñReiniciar ahoraò***.
  - El equipo procederá a reiniciarse, una vez listo haga clic en ***ñOpciones avanzadasò > ñConfiguraci· n de inicioò > ñReiniciarò*** y
  - Seleccione ***ñModo seguro con funciones de redò***.

- Para **usuarios de Windows 10:**
  - Presione el botón de ***ñWindows ( )ò***, en la barra de búsqueda escriba ***ñOpciones de recuperaci· nò***,
  - Luego en el apartado de Inicio avanzado haga clic en ***ñReiniciarò***.
  - El equipo procederá a reiniciarse, una vez listo haga clic en ***ñSolucionar problemasò > ñOpciones avanzadasò > ñConfiguraci· n de inicioò > ñReiniciarò*** , y
  - Seleccione ***ñModo seguro con funciones de redò***.

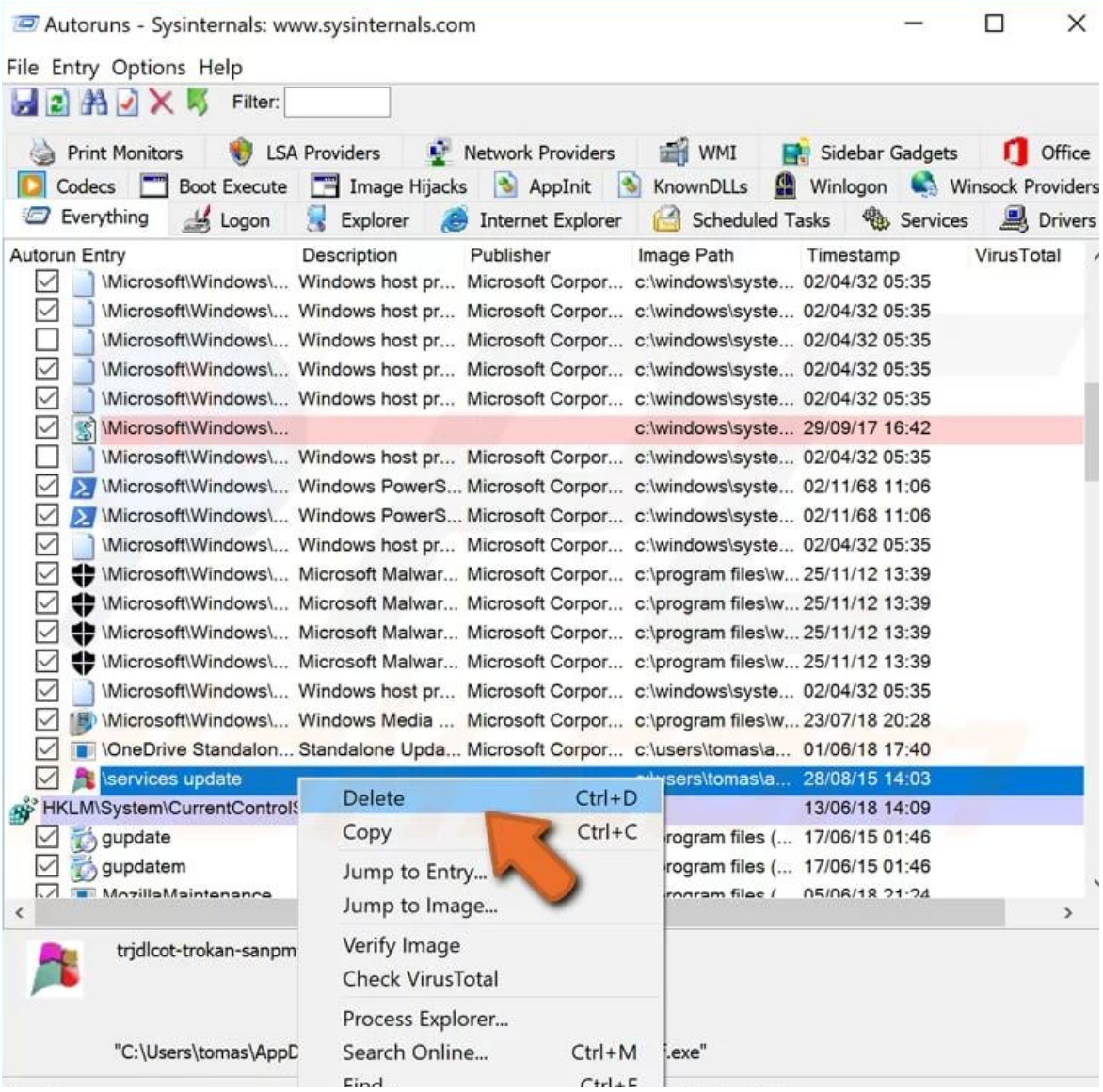
- Una vez haya iniciado su equipo en modo seguro, extraer el archivo descargado (Autoruns) y ejecutar el archivo ***Autoruns.exe***.



- En la aplicación ***ñAutorunsò***,
  - Haga clic en ***ñOpcionesò*** y desactive las opciones ***ñOcultar ubicaciones vac²asò*** y ***ñOcultar entradas de Windowsò*** y
  - Luego haga clic en el icono ***ñActualizarò***.



- Consultar la lista provista por la aplicación ***ñAutorunsò*** y localizar el proceso de malware que desea eliminar, en este caso el **"WindowsFormsApp2"** y el **"Журналы и оповещения производительности.exe**.



- Una vez haya eliminado el proceso asociado al malware, buscar el archivo malware en su computadora, para ello puede hacer verificar el apartado de ***ñImage Pathò*** del proceso, allí le indicará la ubicación del archivo malware. Cuando localice el archivo malware asegúrese de eliminarlo completamente del sistema.