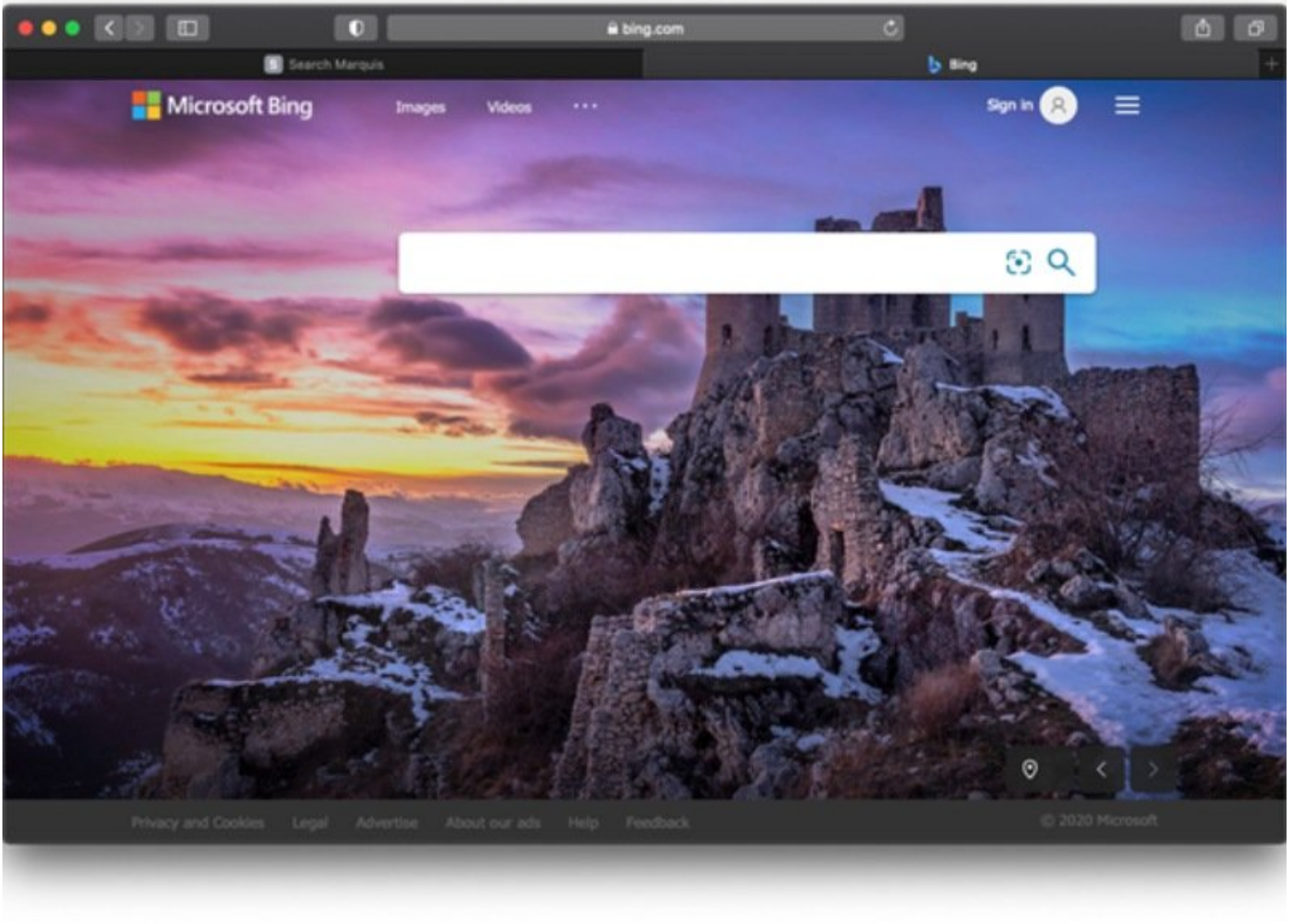
Cómo eliminar del Mac el malware de redireccionamiento de Bing.

Los siguientes pasos le ayudarán a eliminar el malware de Mac que pone en marcha la molesta actividad de redireccionamiento.

Escrito por: David Balaban



INTRODUCCIÓN

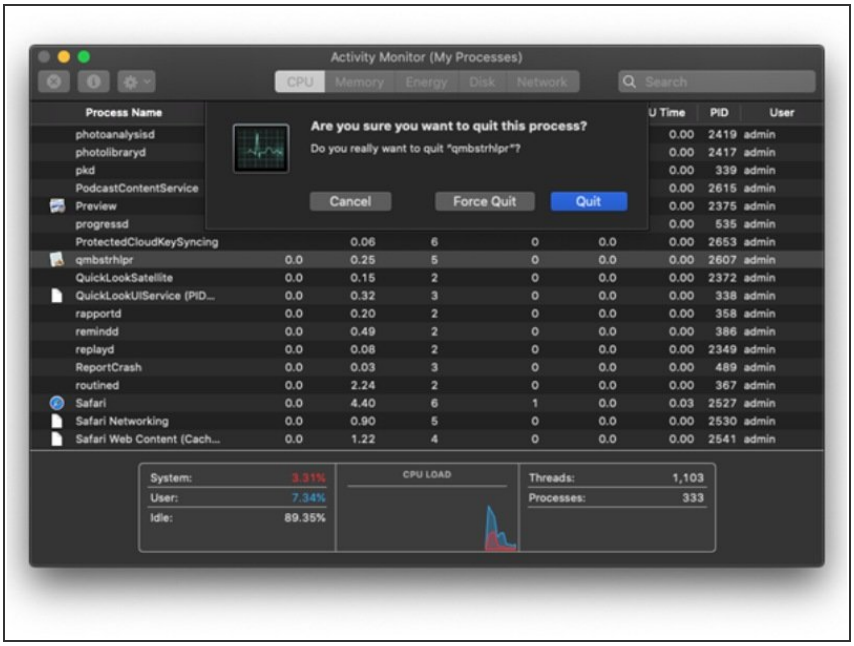
Dicen que las Mac no contraen virus. Probablemente sea cierto, siempre y cuando se ciña a la definición tradicional de virus informático como un programa malicioso que se replica dentro de un sistema. Sin embargo, las Mac reciben toneladas de malware y adware de gran variedad.

El artículo Bing redirect amenaza y demuestra lo prolífica que puede llegar a ser una sola cepa de malware para Mac en estos días. Secuestra los navegadores web de una víctima, incluidos Safari, Google Chrome y Mozilla Firefox, y los redirige a Bing.com a través de una serie de URL auxiliares como *'SearchMarquis.com'* y '' 'SearchBaron.com' ' '.

La lógica detrás de esta extraña toma de control del navegador es dirigir silenciosamente el tráfico a través de redes publicitarias de mala reputación antes de que llegue a Bing. Si bien el papel de este motor de búsqueda legítimo es ocultar el juego sucio, es el síntoma principal del ataque.

Si está experimentando este problema, los siguientes pasos lo ayudarán a eliminar el malware de Mac que activa la molesta actividad de redireccionamiento.

Paso 1 — Terminar el proceso malicioso

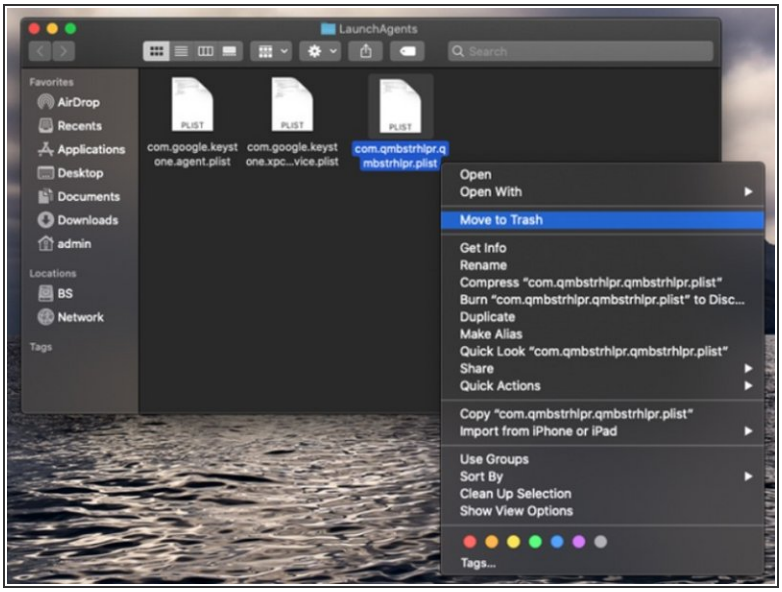


- Haga clic en el botón Ir en la barra del Finder de su Mac, seleccione Utilidades en la lista desplegable y abra el Monitor de actividad.
- Intente detectar el proceso malicioso. Concéntrese en los ejecutables que generan múltiples subprocesos, tienen íconos que no reconoce y usan una cantidad significativa de CPU y memoria.
- Si encuentra el proceso malicioso, haga clic en el botón X en la parte superior derecha de la aplicación Monitor de actividad y luego seleccione la opción Salir o Forzar salida en el cuadro de diálogo de seguimiento.

Paso 2 — Desinstale la aplicación no deseada

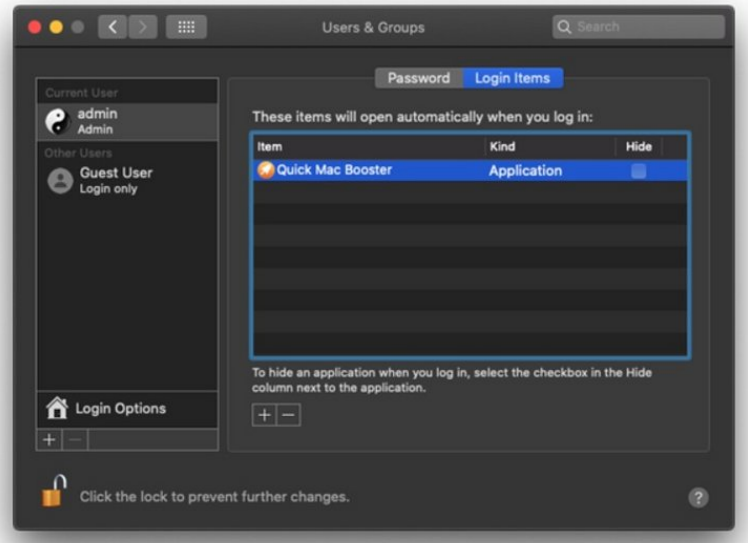
- Vuelva a expandir el menú Ir en el área del Finder y seleccione Aplicaciones. Consulte la lista de una aplicación que haya aparecido recientemente en su Mac sin su permiso. Mueva al culpable a la Papelera.

Paso 3 — Borrar LAunchAgents maliciosos



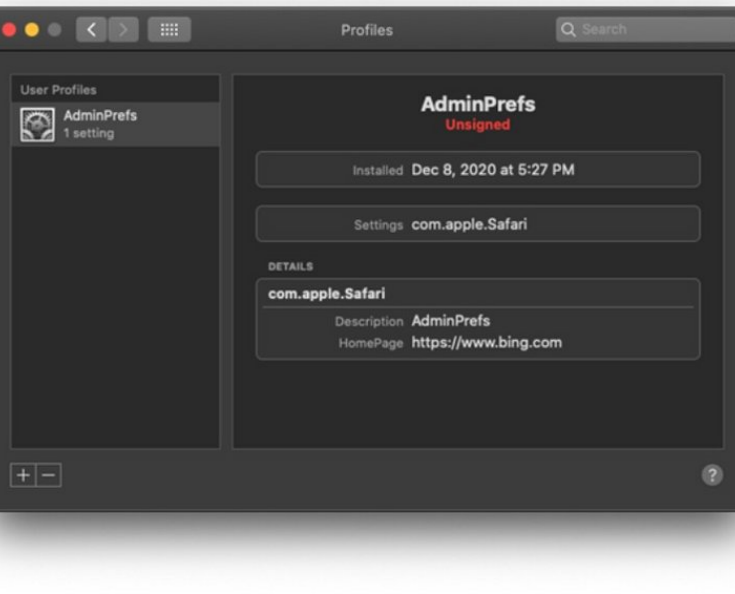
- Seleccione la opción Ir a la carpeta como se muestra a continuación.
- Ingrese ~ / Library / LaunchAgents (con el signo de tilde) y haga clic en Ir.
- Verifique la ruta de LaunchAgents en busca de archivos dudosos agregados recientemente y elimínelos.
- Utilice la función Ir a la carpeta para abrir las siguientes rutas: / Library / LaunchAgents (sin el signo de tilde), / Library / LaunchDaemons y ~ / Library / Application Support. Revise su contenido y mueva los archivos y carpetas sospechosos a la Papelera.

Paso 4 — Elimine elementos de inicio de sesión poco fiables



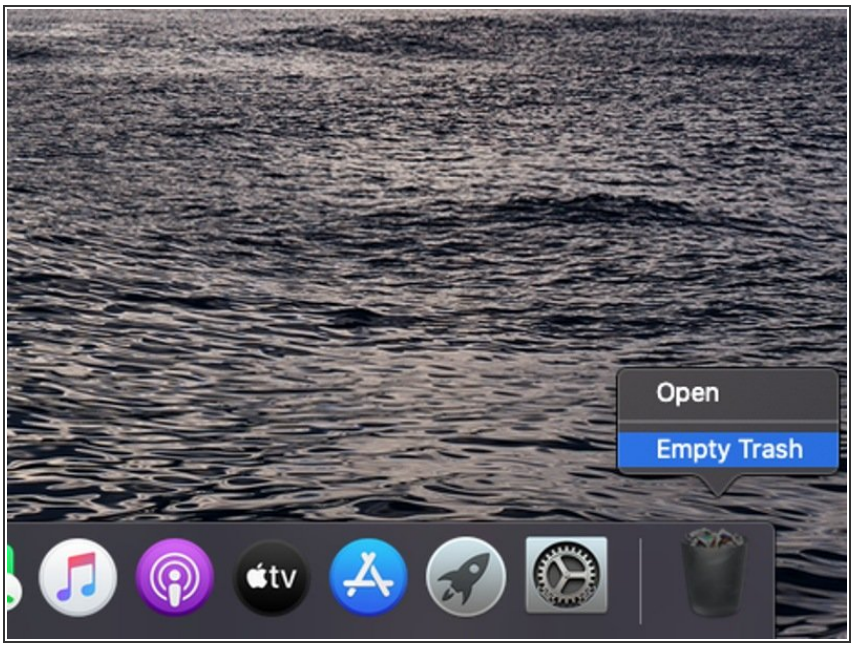
- Vaya a Preferencias del sistema, seleccione Usuarios y grupos y haz clic en la pestaña Elementos de inicio de sesión. Para realizar cambios, deberá hacer clic en el icono del candado en la parte inferior izquierda y escribir su contraseña. Luego, seleccione la aplicación maliciosa y haga clic en el signo "menos" para eliminarla de la lista.

Paso 5 — Eliminar el perfil de configuración no autorizado



- Vaya a Preferencias del sistema y seleccione Perfiles. Tenga en cuenta que esta función faltará si no hay perfiles de dispositivo instalados en su Mac. Sin embargo, si aparece en la lista, ábralo, seleccione el perfil no deseado y haga clic en el signo "menos" para deshacerse de él.

Paso 6 — Vacíe la papelera

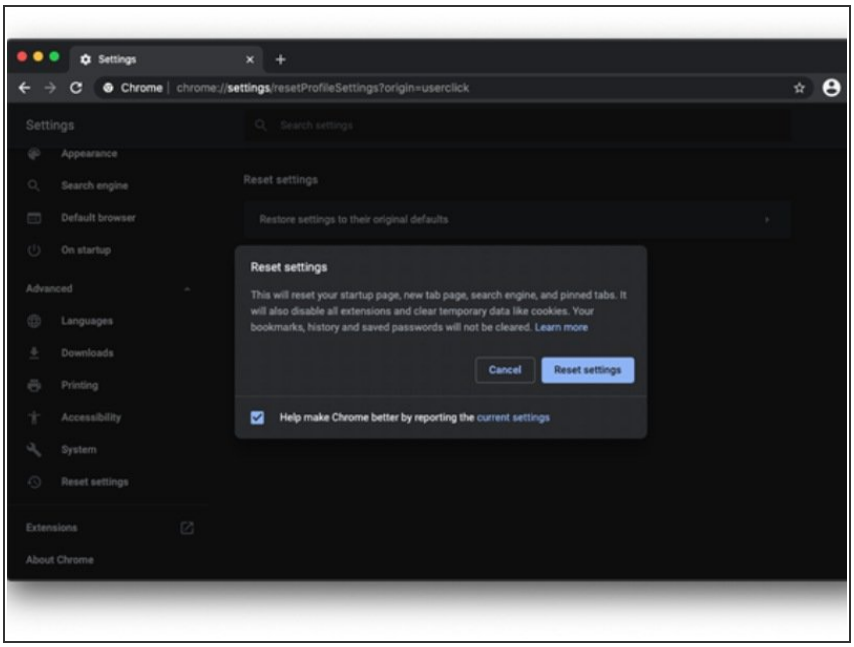


- Mantenga presionada la tecla Control y haga clic en el ícono de la Papelera en el Dock de su Mac, seleccione Vaciar Papelera en el menú contextual y haga clic en el botón Vaciar Papelera en el cuadro de diálogo de seguimiento para confirmar esta acción.

Paso 7 — Limpie datos redundantes en Safari

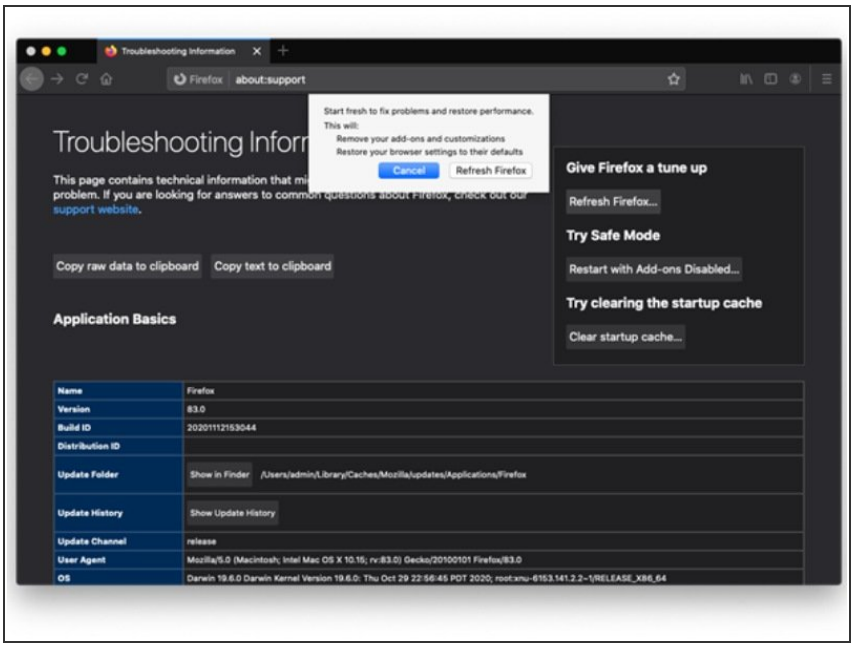
- Abra el navegador web, expanda el menú desplegable **Safari** en la barra del Finder y seleccione Preferencias. Haga clic en la pestaña Avanzado y coloque una marca de verificación junto a la opción que dice **Mostrar menú Desarrollar en la barra de menú** (si aún no está habilitado).
- Ahora que el menú **Desarrollar** se muestra en el área del Finder, haga clic en él y seleccione *Vaciar cachés* como se ilustra a continuación.
- Expanda el menú **Historial** y seleccione *Borrar historial*. Haga clic en el botón *Borrar historial* en el cuadro de diálogo de confirmación.
- Vuelva a abrir la pantalla Preferencias de Safari, haga clic en la pestaña *Privacidad* y seleccione *Administrar datos del sitio web*. Haga clic en el botón *Eliminar todo* para eliminar todos los bits y piezas de información que los sitios web han almacenado para rastrear sus actividades en línea. Luego, haz clic en el botón Listo.
- Reinicie Safari

Paso 8 — Restablezca Google Crhome (si le afecta)



- Abra Chrome, haga clic en el botón Personalizar y controlar Google Chrome y seleccione Configuración.
- Haga clic en el botón Avanzado en la barra lateral y desplácese hacia abajo hasta Restablecer configuración. Seleccione la opción Restaurar la configuración a sus valores predeterminados originales y haga clic en Restablecer configuración.
- Reinicie Crhome

Paso 9 — Restablezca Mozilla Firefox (si le afecta))



- Abra Firefox, haga clic en el botón de menú Abrir, vaya a Ayuda y seleccione Información de solución de problemas.
- Haga clic en el botón Actualizar Firefox y confirme la acción una vez que aparezca un cuadro de diálogo de seguimiento.
- Reinicie Firefox

Para evitar que Bing redireccione el malware en el futuro, utilice los instaladores de aplicaciones con precaución, especialmente a los que se descargan de mercados de software no oficiales. Esta infección depende principalmente de los paquetes de aplicaciones para propagarse. La opción de instalación predeterminada ("rápida") solo menciona el software benigno y nunca revela la estructura real de dichos paquetes. Como resultado, los usuarios hacen clic sin pensarlo dos veces, descubren en breve que sus navegadores web están siendo controlados.