CLAVES PARA ACTUAR FRENTE AL ATAQUE DE RANSOMWARE WANNACRY

ÍNDICE

¿Qué es WannaCry?, ¿Cómo puedo saber si he sido infectado?

Se trata de un ataque ransomware que ha afectado principalmente a entornos corporativos, y tiene la particularidad de que una vez infecta a un equipo comienza a propagarse por la red realizando conexiones al puerto 445 (SMB). WannaCry utiliza código para explotar una vulnerabilidad publicada por Microsoft el día 14 de marzo en el boletín MS17-010.

En estos momentos contamos con herramientas de seguridad capaces de detectar si se ha sido objeto de este ataque.

Para conocer cómo analizar el equipo fuera de línea antes de conectar el equipo, consultar estos pasos.

Para conocer cómo analizar el equipo con la solución de centralANTIVIRUS instalada en el equipo, consulte estos pasos.

He sido infectado, ¿cómo puedo actuar?

Como en cualquier otra variante de ransomware, si se ha sufrido una infección los archivos han sido encriptados, no es posible revertir el estado de los archivos a su estado original mas allá de mediante la restauración de copias de seguridad. Nuestra recomendación en este caso es analizar el equipo para limpiar los archivos originarios de la infección y recuperar los archivos de copia de seguridad.

Recomendación: Contacte con nuestros expertos en seguridad para que puedan asesorarle acerca de la solución más adecuada de seguridad para su entorno.

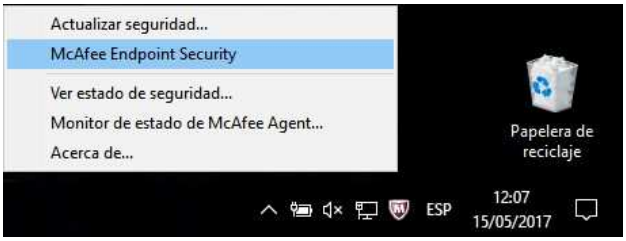
Pasos a seguir para analizar el equipo que ha sido encriptado:

1. Analizar el equipo completamente con su solución antivirus instalada en el equipo.

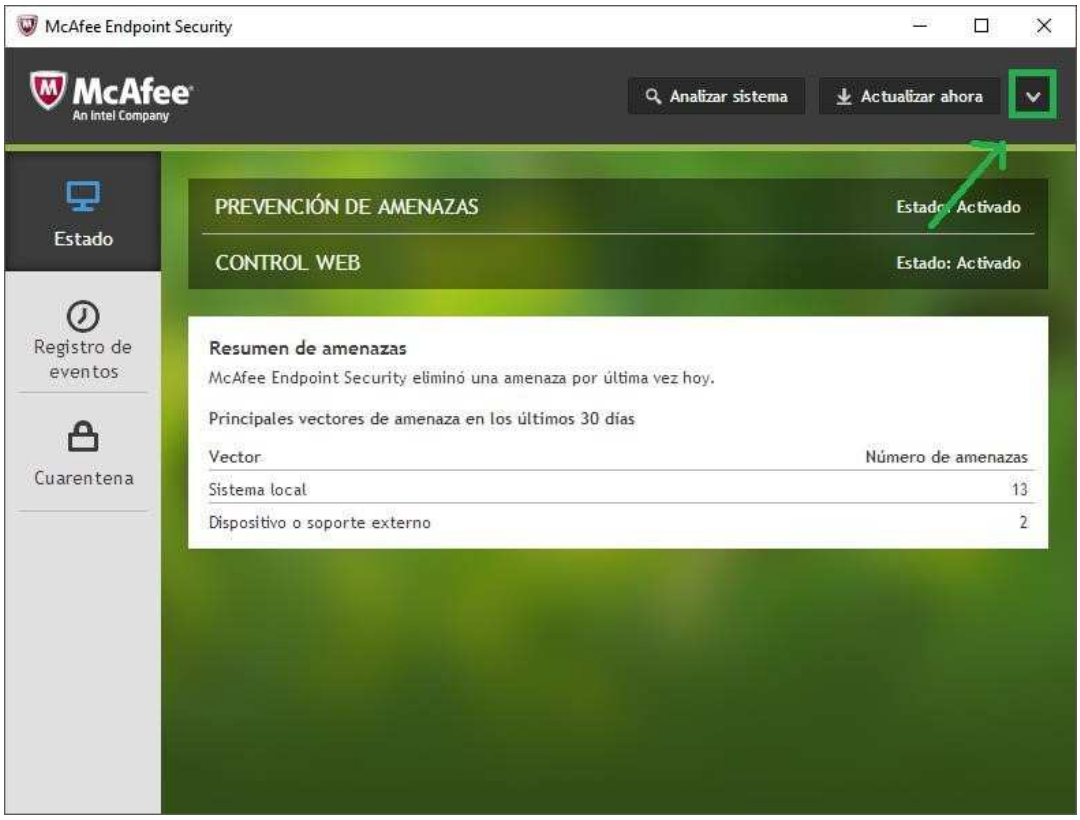
2. Recuperar los archivos de copia de seguridad.

Si dispone de la protección de centralANTIVIRUS.com, siga los pasos descritos a continuación:

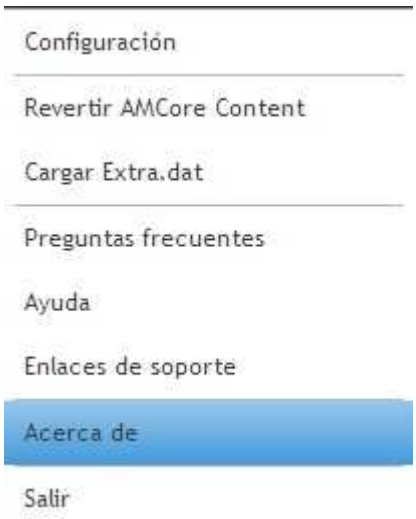
1. Dirigirse localmente en el equipo al icono de McAfee, hacer clic con el derecho del ratón y seleccionar: McAfee Endpoint Security.



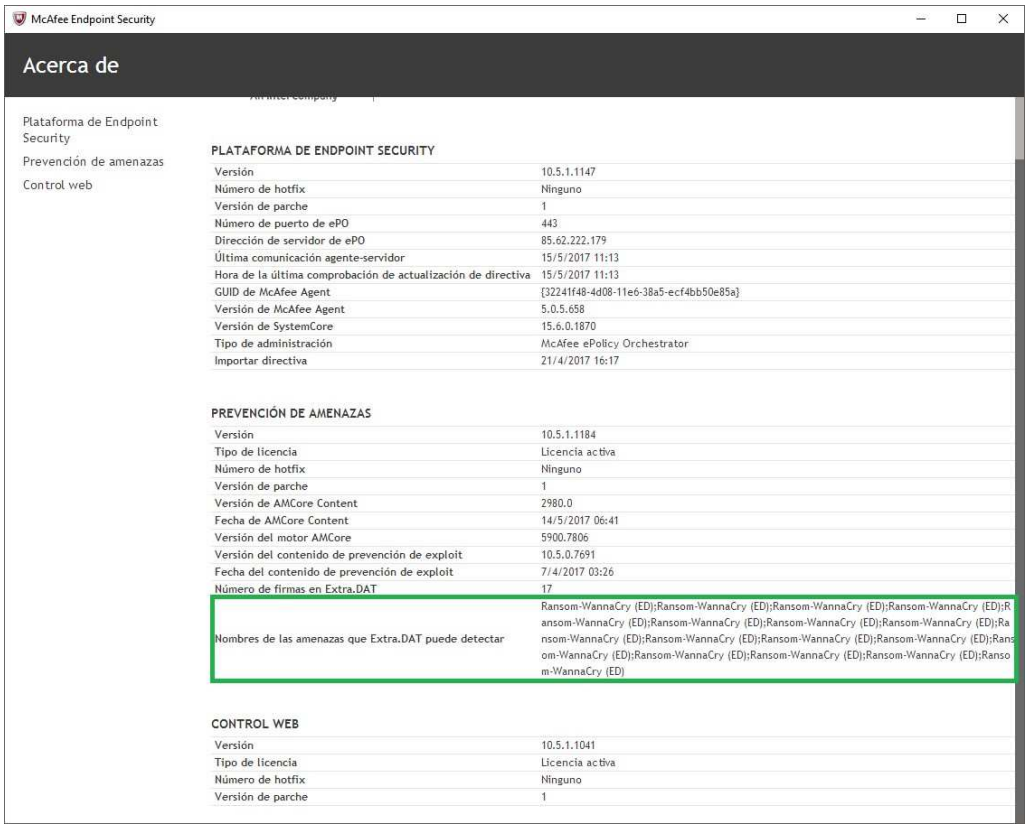
2. Dirigirse al desplegable menú como se observa en la siguiente imagen.



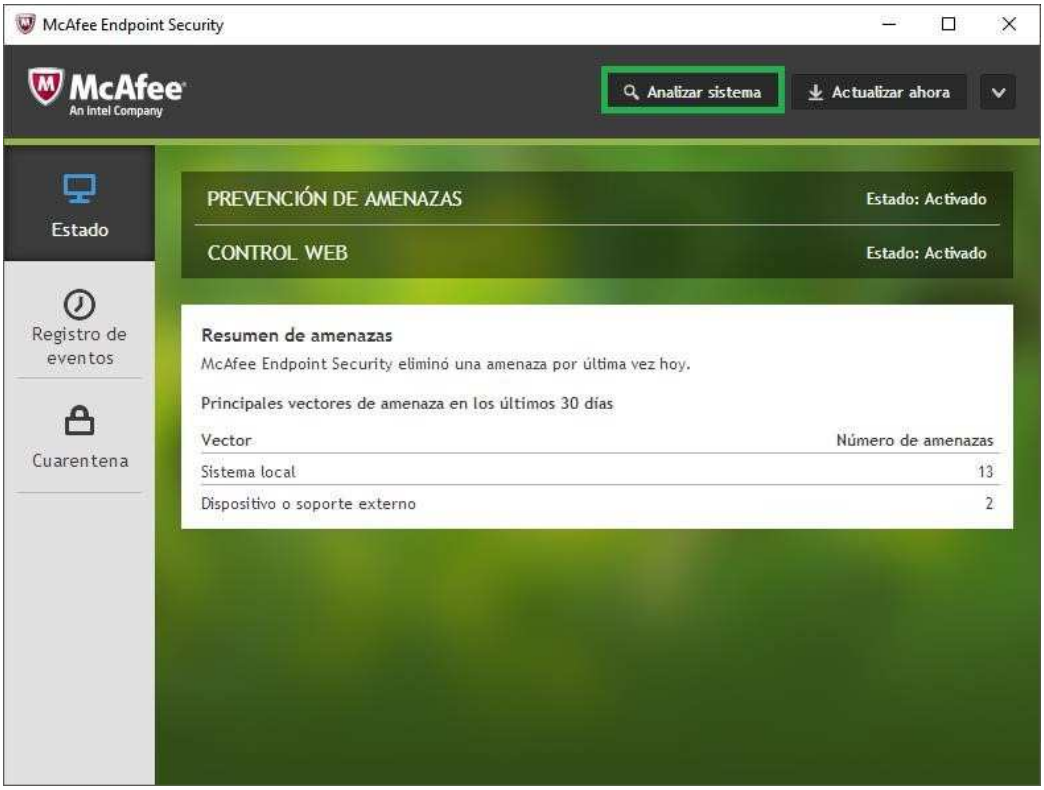
3. Seleccionar en el menú la opción "Acerca de"



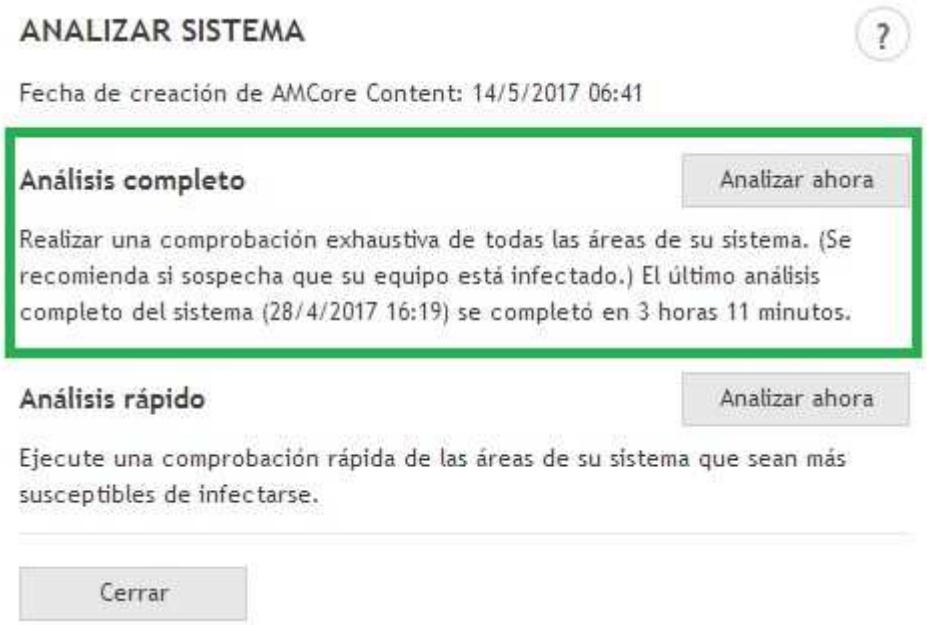
4. Comprobar si se dispone de la siguiente actualización:



5. Volver a la pantalla anterior y pulsar sobre el botón "Analizar sistema"



6. A continuación, buscar "Análisis Completo" y hacer clic sobre el botón "Analizar ahora"



Esperar a que finalice el análisis y comprobar los resultados. Si se detectan archivos pertenecientes a la familia del ransomware WannaCry serán movidos a cuarentena directamente durante el análisis.

Si dispone de otras soluciones de seguridad, por favor contacte con Lidera Network.

No sé si he sido infectado. ¿Puedo encender mis equipos con normalidad?

El ransomware WannaCry comenzó a propagarse la mañana del viernes 12 de Mayo. Desde entonces se han habilitado diferentes actualizaciones que evitan la infección y propagación de este ransomware.

Si sospecha que ha podido ser atacado y no sabe como actuar o no se quiere arriesgar a encender sus equipos, le recomendamos analizar el equipo antes de conectarlo a la red. Y para ello le explicamos a continuación cómo proceder: Contamos con herramientas de análisis para ejecutarse en modo seguro sin funciones de red capaces de limpiar los equipos infectados con WannaCry.

Pasos a seguir para analizar los equipos en modo seguro:

1. Iniciar el sistema en modo a prueba de fallos sin funciones de red. Para ello, pulsar la tecla F8 repetidas veces durante el arranque.

2. Ejecutar la herramienta Stinger en función de la arquitectura del sistema operativo:

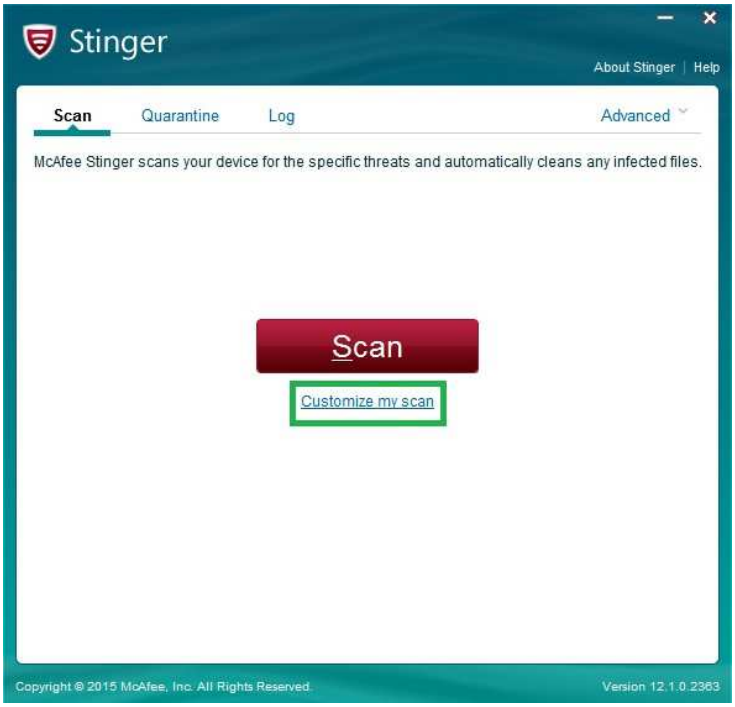
***32bits:**

http://canal.lidera.com/es/download/files/Stinger_x32.zip

***64bits:**

http://canal.lidera.com/es/download/files/Stinger_x64.zip

3. Una vez abierta la herramienta Stinger, seleccionar la opción "customize my scan" y seleccionar todo el equipo.



4. Pulsar el botón Scan y esperar hasta que finalice el análisis.

5. Una vez el análisis haya terminado, reiniciar el sistema normalmente.

6. Recomendación importante - Aplicar todas las actualizaciones del sistema operativo.