UT01: Adopción de pautas de seguridad informática - Vulnerabilidades

Nombre: Francisco Jesús García – Uceda Díaz - Albo
Curso: 2º ASIR.

Índice

b) Realiza un breve informe sobre vulnerabilidades en sistemas operativos Microsoft y utiliza alguna herramienta de detección de vulnerabilidades Microsoft en alguno de sus productos.

Microsoft es una gran empresa reconocida en todo el mundo hoy en día, pero en estos últimos años destaca sobre todo por un tema que engloba a todas las empresas, las vulnerabilidades. Bien es sabido hasta por las personas con menos conocimiento sobre esto que Microsoft con su sistema operativo Windows 10 carece de muchos fallos en los últimos años y que además estos están saliendo a la luz, los agujeros de seguridad.

Cada mes Windows lanza el conocido Patch Tuesday o martes de actualización el cual corrige un buen montón de vulnerabilidades encontradas. Una de estas vulnerabilidades ha sido identificada como CVE-2019-1367 el cual aprovecha un fallo en el navegador de Internet Explorar para escalar privilegios en Windows, pudiendo así tomar el control total del ordenador.

Otra de las vulnerabilidades crítica que corrige este parche es la identificada como CVR-2019-1255, se trata de un fallo en Windows Defender que puede ser explotado por un atacante dejando nuestro equipo totalmente desprotegido.

A pesar de que Windows ha corregido ya estas dos vulnerabilidades críticas es muy normal escuchar ya esto de Microsoft y sus fallos de vulnerabilidad en sus sistemas operativos Windows.

Podemos remontarnos al mes anterior de agosto el cual se corrigió 'in extremis' una importante vulnerabilidad catalogada como crítica, el autor de esta la bautizo como BlueKeep y están identificadas como CVE-2019-1181 y CVE-2019-1182. Esta vulnerabilidad afecta directamente al escritorio remoto.

Un posible atacante podría desplegar malware a un equipo vulnerable sin que la víctima tuviera que intervenir. Todo de forma remota. Según el autor de descubrir la vulnerabilidad (el cual trabaja para Microsoft) esta vulnerabilidad no habría sido explotada por ninguna persona.

En caso de tener éxito y lograr explotar estas vulnerabilidades, un atacante ganaría acceso total al sistema. Podría ejecutar código arbitrario que comprometería seriamente la seguridad y la privacidad de los usuarios. Por ejemplo, podría instalar software diseñado para recopilar todo tipo de datos, robar información, crear cuentas en determinadas plataformas, etc.

Para rematar todo esto podemos irnos a Julio el cual Microsoft nada más y nada menos corrigió 77 vulnerabilidades y entre ellas un 0-day, este 0-day se aprovecha de un fallo grave en Windows para obtener privilegios y así poder ejecutar código arbitrario.

Para finalizar el informe compararemos todas las vulnerabilidades registradas en Windows en todo el 2018. La CVE en todo 2018 recopilo 16.029 vulnerabilidades en Windows, un 9% más que en 2017, esto si echamos cuentas con 46 vulnerabilidades reportadas a día.

No todos son malas noticias para Windows y es que si es cierto que son muchas vulnerabilidades, en la tabla que publica la CVE en su web oficial (link) Windows está en décimo lugar. El primer puesto lo tiene Debian seguido de Ubuntu, Android y teniendo el 4º, 5º y 6º distribuciones empresariales de Linux.

Los fabricantes con más vulnerabilidades en 2018 fueron Debian (823), Oracle (690) y Microsoft (664), mientras que las aplicaciones con más vulnerabilidades fueron Firefox (333), Acrobat DC y Acrobat Reader DC (285) y PhantomPDF (223). Con esto en cuenta, los fabricantes con el promedio de criticidad de vulnerabilidades más alto en la historia son Adobe (8,80), Qualcomm (8,50) y RealNetworks (8,50), mientras que aquellos con más vulnerabilidades históricamente resultan Debian (823), Oracle (690) y Microsoft (664).

Los tipos de vulnerabilidades más frecuentes en 2018 fueron la ejecución de código (23%), ataques de overflow (18%) y de XXS (15%). Aún más, el 79% de las vulnerabilidades de ejecución de código eran graves (puntaje de criticidad mayor o igual a siete).

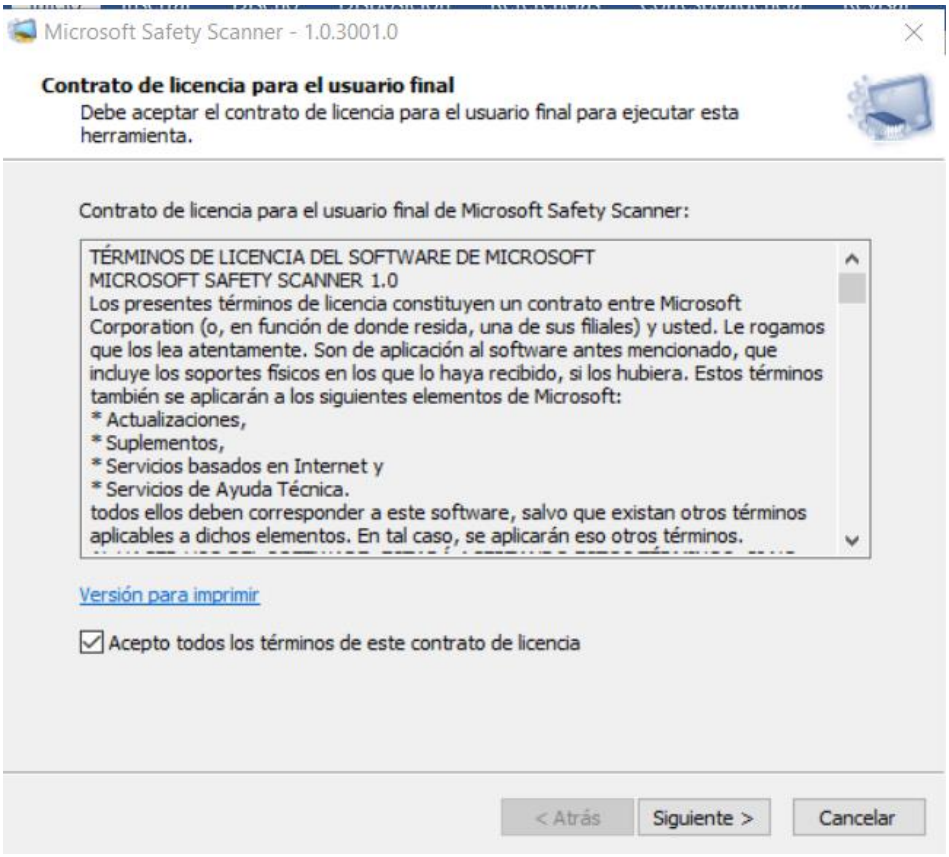
Herramientas de Microsoft para detección de vulnerabilidades.

Microsoft Safety Scanner (Link).

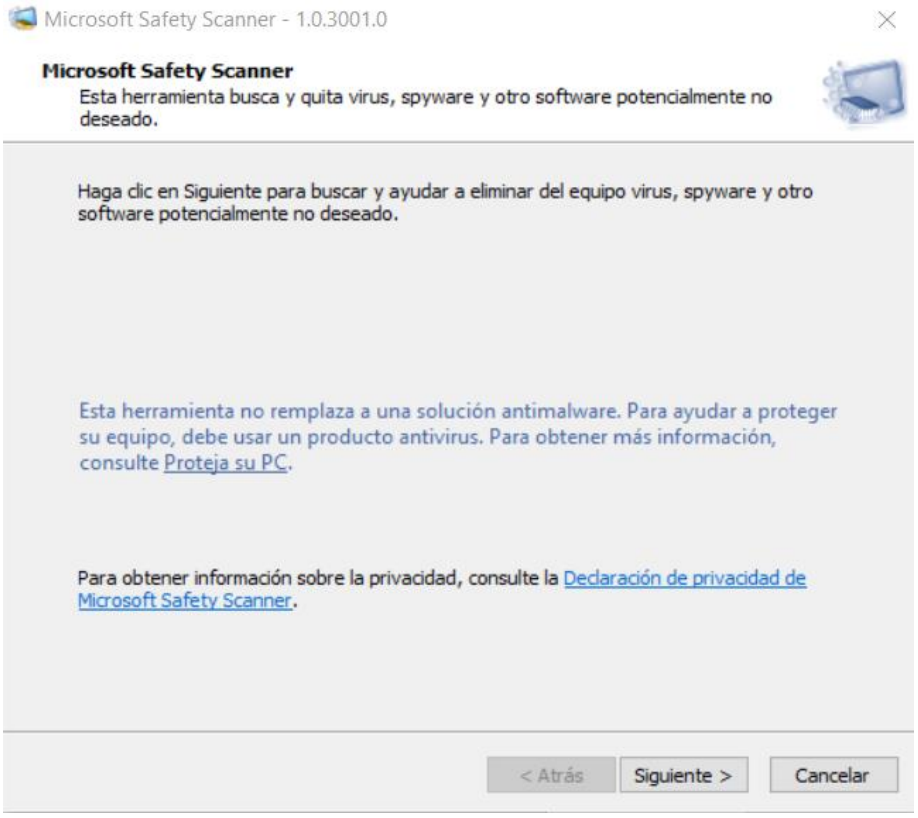
Microsoft Safety Scanner es una herramienta desarrollada por Microsoft, similar a la herramienta de eliminación de software malintencionado de Windows, que sirve para analizar la computadora en busca de virus. Wikipedia

Una vez descargado lo ejecutamos:

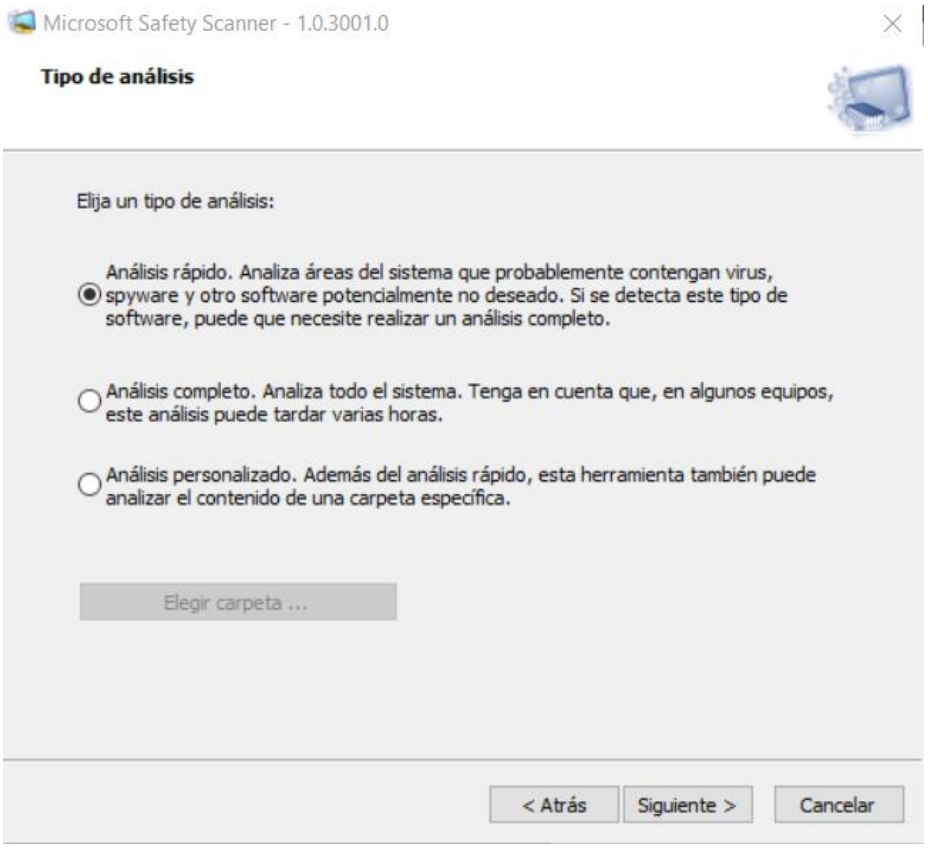
Aceptamos la licencia y pulsamos en siguiente:



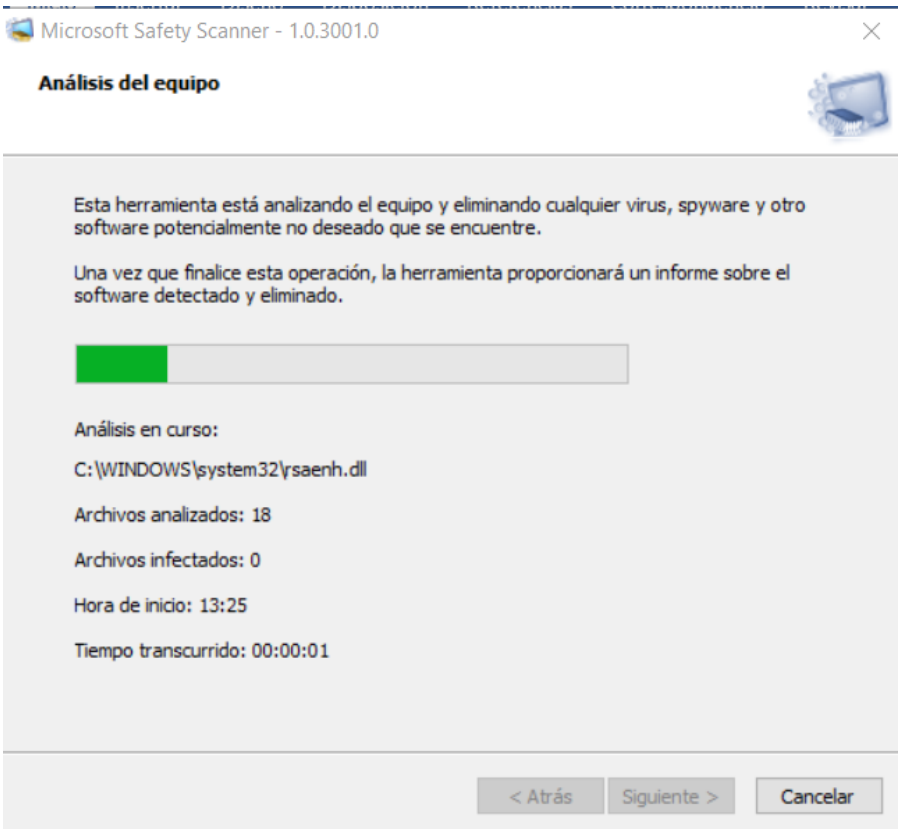
En la siguiente pestaña Microsoft nos dice que esta herramienta no sustituye a un antimalware especializado.



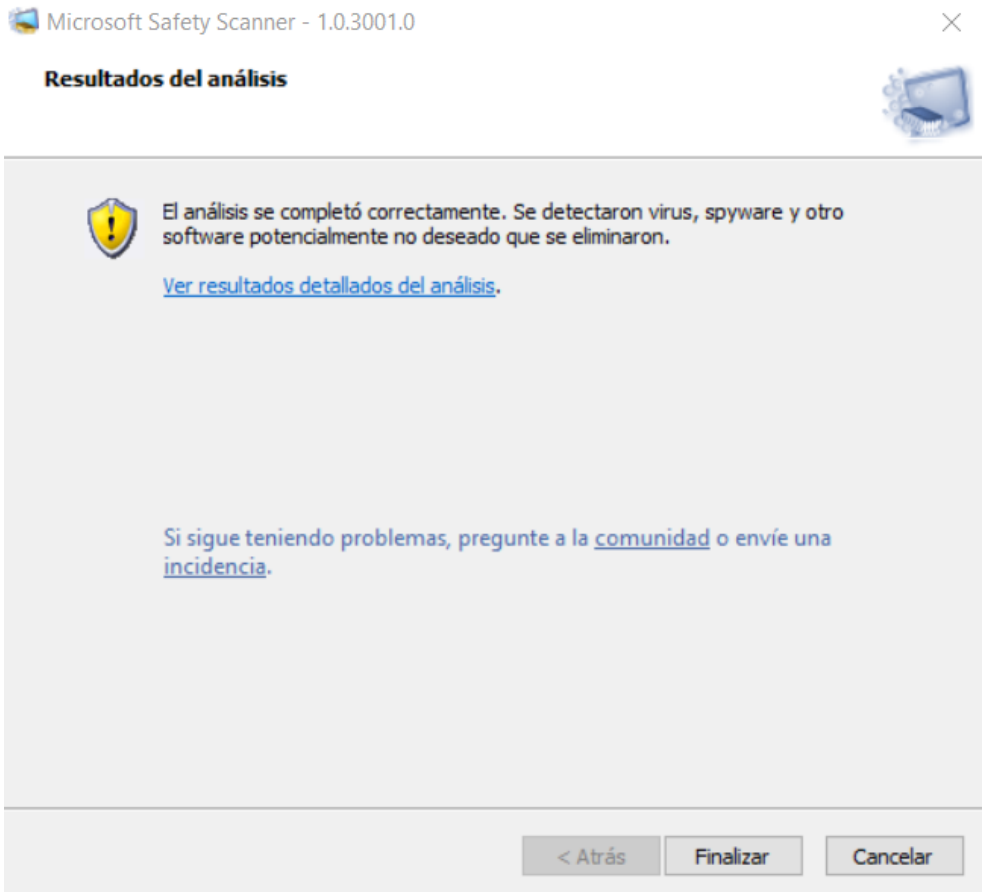
Nos preguntará que análisis queremos ejecutar. Primero haremos un examen rápido.



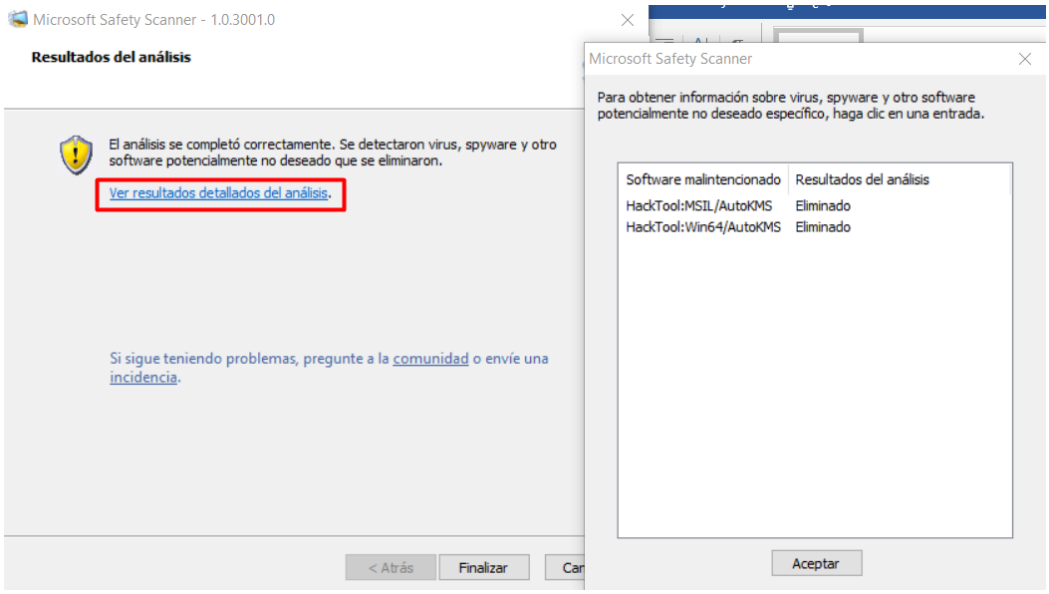
Empezará el análisis, esto tardará algunos minutos:



Una vez finalizado nos dirá un mensaje del resultado, en mi caso se encontraron amenazas pero hay que ver si son falsos positivos o amenazas reales.



Si pulsamos en *'Ver resultados detallados del análisis'* veremos los detalles de los virus encontrados, como vemos en este caso nos eliminó el KMSPico.



Pulsando en Finalizar se cerrará el programa.