Análisis de documentos maliciosos – Parte 04 – Medidas defensivas, próximos pasos y conclusión

Español

Hasta ahora, hemos cubierto una introducción al modelado de amenazas, el uso de máquinas virtuales como entornos para analizar malware y cómo comenzar a analizar documentos PDF y de Microsoft Office en partes anteriores. Todos estos temas nos ayudarán a dar un mejor soporte a otros como primera línea de defensa contra documentos sospechosos.

Sin embargo, si damos soporte a los actores vulnerables (el público principal al que va dirigida esta serie de publicaciones), sabemos que esto es sólo una parte de la historia. También debemos asegurarnos de poder proporcionar un buen asesoramiento proactivo a nuestros beneficiarios, para que estén bien protegidos de los documentos maliciosos antes de que lleguen a sus discos duros. Esperemos que, con todo el contenido revisado, podamos no sólo entender mejor los consejos clásicos que damos a los usuarios finales, sino también proponer un par de medidas adicionales que podrían ser útiles para los actores vulnerables con un nivel de riesgo elevado.

La primera idea que queremos reforzar es que decirle a los activistas, periodistas y medios de comunicación que no abran archivos de fuentes desconocidas **no** es un consejo sostenible. Para poder llevar a cabo sus actividades, muchas personas de estas categorías necesitan abrir archivos que les envían y que podrían contener amenazas, como invitaciones a conferencias de prensa, documentos filtrados, agendas de eventos, etc. Por lo tanto, el consejo más pertinente que podemos darles es que conozcan los riesgos y creen procesos que les permitan abrir los archivos de la forma más segura posible.

Habiendo dicho esto, algunas medidas defensivas contra los documentos maliciosos incluyen

En general

Soluciones antivirus

Muchos documentos maliciosos distribuidos son parte de operaciones masivas que están documentadas e integradas con éxito en las bases de datos de detección de antivirus. No olvide que esta recomendación no garantiza la detección de archivos maliciosos diseñados específicamente para objetivos concretos. Aún así, le proporcionará una capa de seguridad que vale la pena tener, especialmente si se trabaja con muchos archivos que no son de confianza. Recuerde elegir un proveedor de confianza, activar la detección en tiempo real si está disponible y mantener actualizada la base de datos.

Mantener el software legal y actualizado

Cada año se descubren y divulgan cientos de nuevas vulnerabilidades para muchos programas de uso diario, incluidos Microsoft Office y los lectores de PDF, y estas

vulnerabilidades se "parchan" mediante actualizaciones de software. Así pues, tener todo el software actualizado reducirá drásticamente las posibilidades de que alguien utilice vulnerabilidades conocidas y documentadas para atacar un objetivo con éxito. Tener software pirateado afectará a su capacidad para detectar y aplicar actualizaciones, convirtiéndolo en un problema de seguridad. Por este motivo, contar con software original es lo más recomendable desde el punto de vista de la seguridad, incluso antes de abordar las consideraciones legales.

Revisar la extensión de los archivos sospechosos

Algunas campañas engañan a los usuarios para que abran archivos dañinos disfrazados de documentos, pero que en realidad son otro tipo de archivos, como aplicaciones ejecutables, archivos .zip u otros tipos de archivos contenedores como .iso, etc. Por lo general, estos archivos incluyen incluso iconos personalizados para que parezcan documentos de MS Word, PDF, etc. Verificar cuidadosamente los archivos que descargamos y abrimos nos dará otra capa de protección al detectar cuando un archivo no tiene un tipo de archivo común o esperado.

Utilizar lectores "prestados"

Una estrategia frecuente consiste en abrir documentos sospechosos en un entorno distinto al de su computadora que esté mejor equipado para detectar y contener cualquier amenaza potencial. Un ejemplo clásico es abrir archivos utilizando Google Drive (esto incluye las vistas previas en Gmail); de este modo, el archivo se abre realmente en los servidores de Google y se renderiza en nuestras computadoras, convirtiendo a Google (o a cualquier otra plataforma con capacidades similares) en el actor que debe preocuparse de las amenazas específicas contenidas en los documentos abiertos. Una desventaja de este enfoque es que perdemos algo de visibilidad y capacidad de análisis, ya que no estamos descargando los archivos, pero será útil para el uso diario.

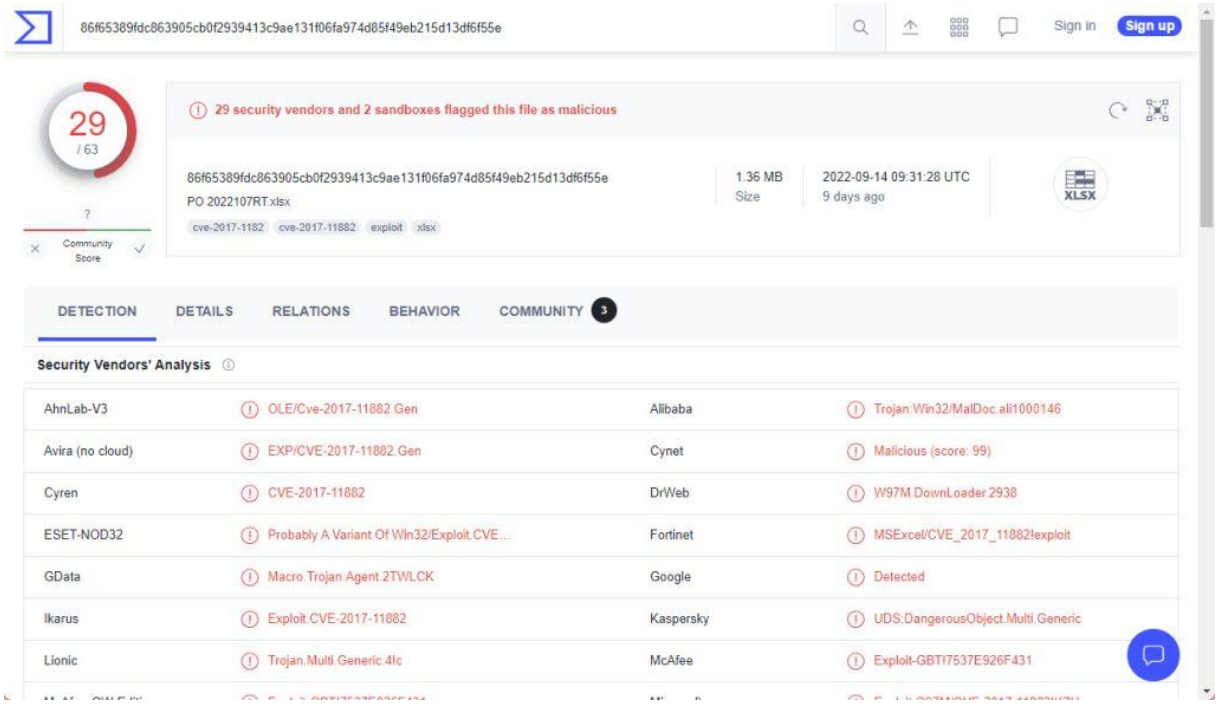
Utilizar herramientas específicas diseñadas para este caso de uso

Existen herramientas que toman el mismo principio de utilizar un entorno seguro para abrir archivos, pero agilizan el proceso para el usuario y luego generan copias seguras que sólo contienen los elementos visibles (similar a imprimir el documento y escanear el resultado en un archivo final). Una de estas herramientas es Dangerzone, un programa que recibe un archivo sospechoso y genera una copia segura para abrirlo. La única desventaja destacable es que la herramienta requiere la descarga de dependencias de algunos GB de tamaño, por lo que si el espacio en el disco duro y/o las velocidades de descarga y la estabilidad son un problema, esta herramienta puede ser más difícil de configurar. Otra herramienta para lograr este objetivo es CIRCLean USB sanitizer de Circl.lu, que usa una computadora separada (proponen una Raspberry Pi) y dos unidades USB. En la primera unidad, se guardan las versiones sospechosas de los archivos, y el software generará las copias seguras y las guardará en la segunda unidad USB. Los desafíos más notables con este enfoque son el uso de hardware dedicado para operar los archivos y los pasos físicos adicionales para mover archivos hacia y desde las unidades USB.

Verificar hashes de archivos en plataformas de detección

Otra estrategia común frente a archivos sospechosos, es verificar en plataformas como VirusTotal si el archivo es conocido como malicioso. Esto nos ayudará a ahorrar tiempo en caso de que el archivo sea una amenaza conocida e incluso nos dará información más valiosa, como qué tipo de malware intenta ejecutar y mensajes de miembros de la comunidad asociados con el archivo. Una observación muy importante es saber que subir el archivo a herramientas como VirusTotal pondrá el archivo a disposición de la comunidad, revelando el contenido del documento (que podría tener información delicada), y alertando potencialmente a los creadores del documento si están monitorizando el archivo específico. Una solución alternativa para esto es no subir el archivo, pero sí verificar su hash. En la primera parte de esta serie, encontrará una guía sobre cómo verificar hashes.

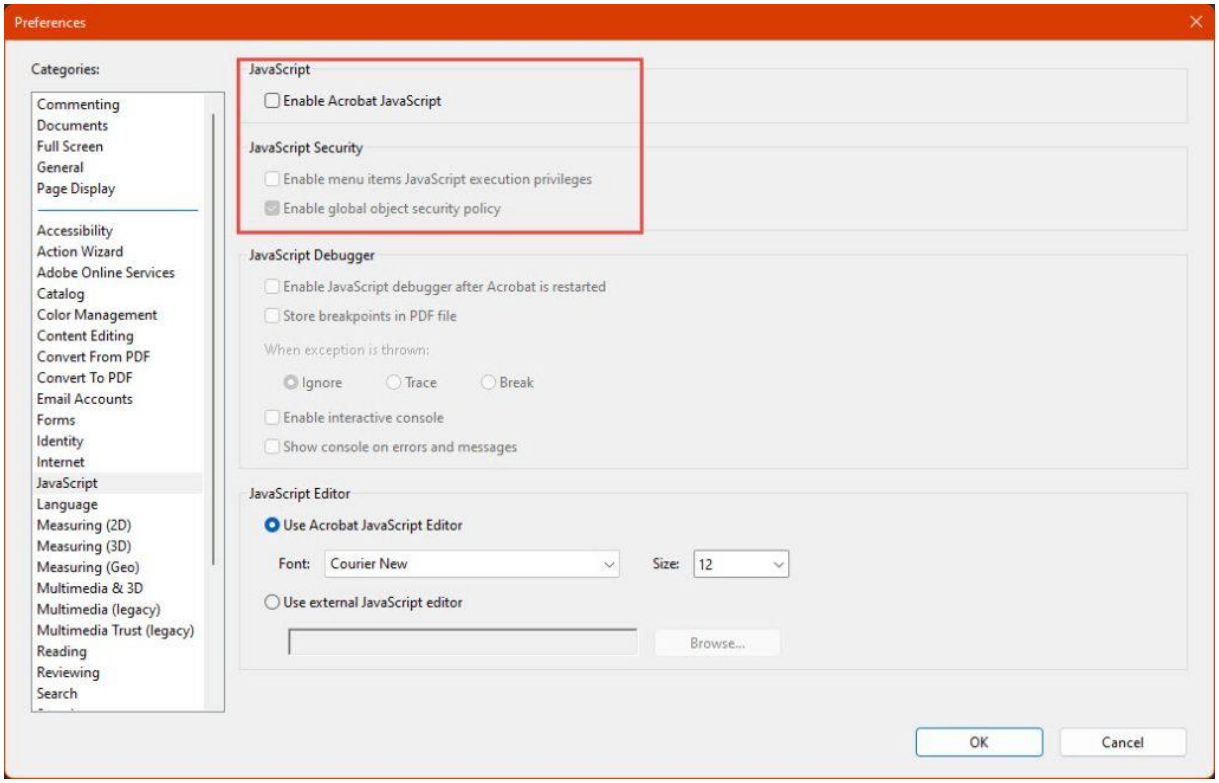
Ejemplo de búsqueda del hash de un archivo, agosto de 2022



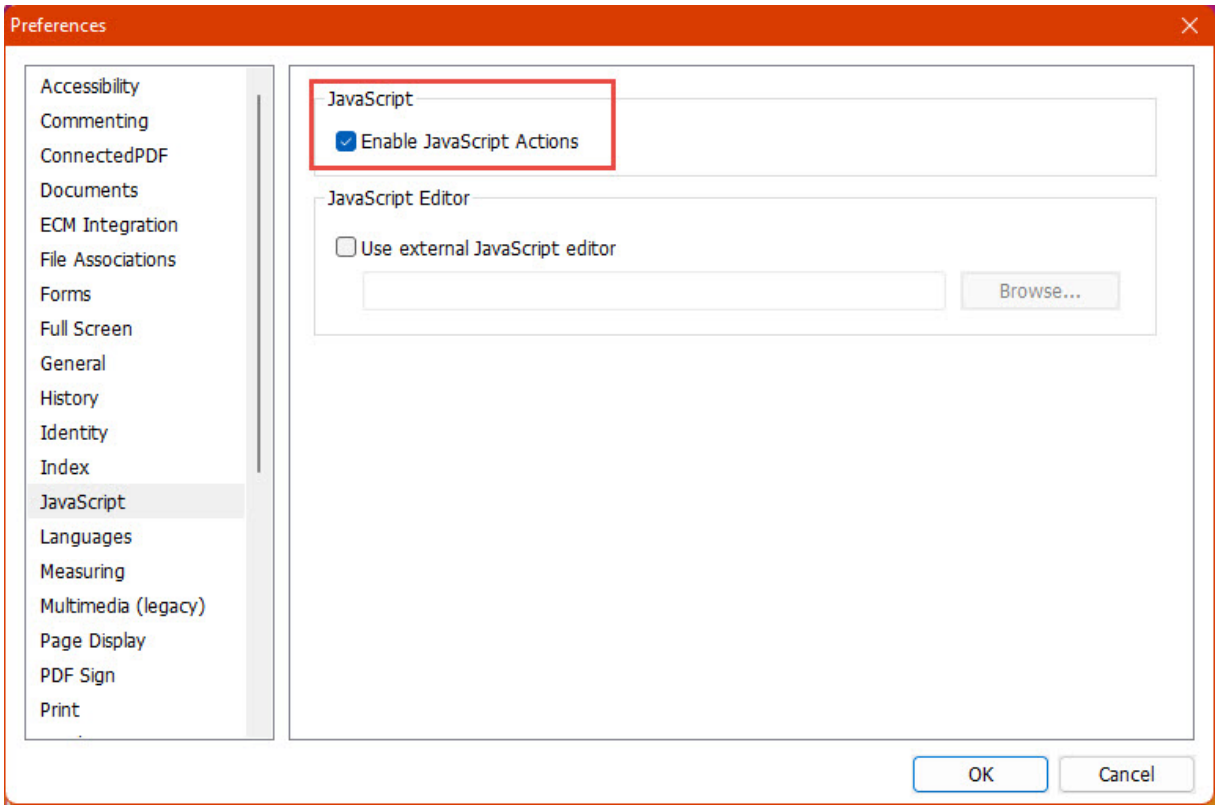
Ejemplo de resultados en VirusTotal, agosto de 2022

Específico para PDF: Deshabilitar la ejecución de Javascript en el lector (y otros ajustes de seguridad)

Dependiendo del software lector de PDF, la ejecución de código JavaScript podría estar ya deshabilitada. Sin embargo, se recomienda volver a verificar en caso de que espere abrir archivos sospechosos. Además, dependiendo de su lector, puede haber otras características de seguridad que puedan configurarse.



Ejemplo para Acrobat Reader (agosto de 2022, Menú Editar -> Preferencias -> Javascript)



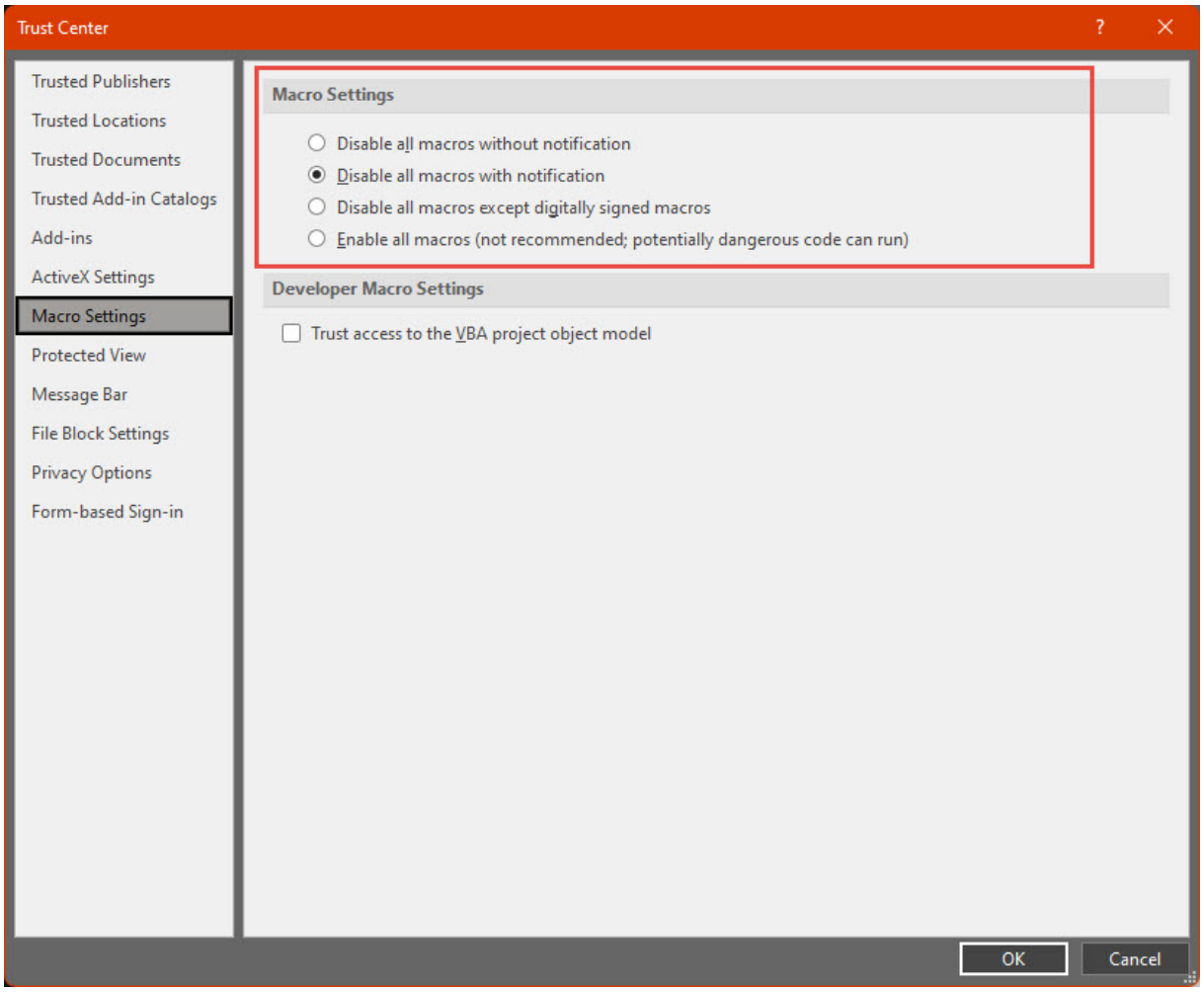
Ejemplo para Foxit Reader (agosto de 2022, Menú Archivo->Preferencias->Javascript)

Específico para Office: Minimizar el uso de macros en actividades legítimas

Aunque existen muchos casos de uso aceptables e inofensivos para las macros, utilizar documentos que las incluyan con frecuencia y estar acostumbrado a habilitarlas, podría abrir la puerta a recibir un documento malicioso y habilitar sus macros accidentalmente. Sobre todo las organizaciones deberían ser conscientes de esta situación y planificar en consecuencia, ya sea eliminando el uso de macros o preparando los procesos para convivir con ellas, tomando en consideración cómo manejar archivos que no sean de confianza.

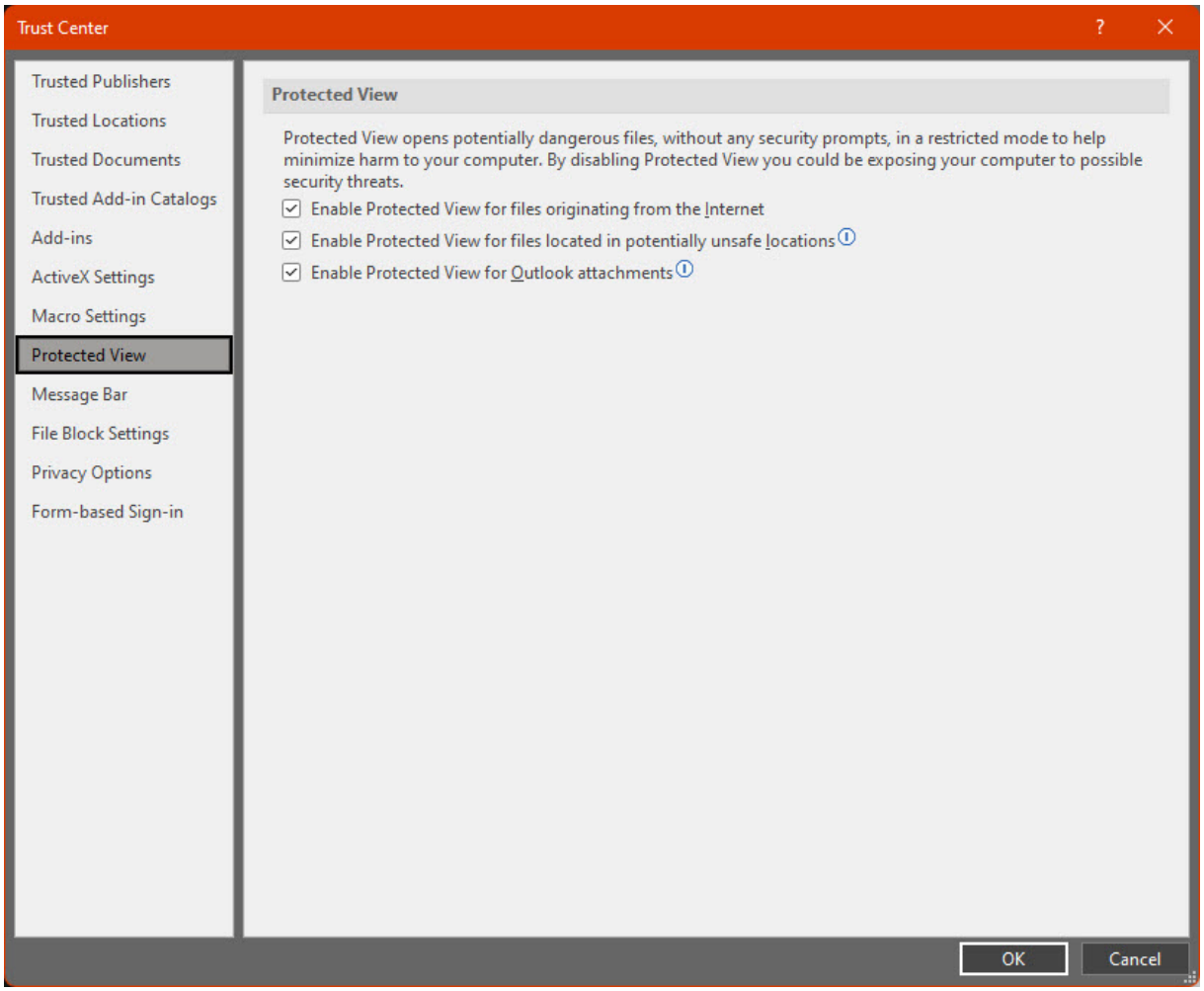
Específico para Office: Deshabilitar las macros y verificar el Centro de Confianza

Hace poco, Microsoft Office cambió varias veces su política sobre las macros, por lo que, dependiendo de cuándo esté leyendo este material, es posible que Office tenga las macros habilitadas o deshabilitadas por defecto. Además, es posible que existan reglas en función del origen de los archivos, etc. Una forma de tener más visibilidad y control es verificar el Centro de Confianza para observar y configurar directamente el comportamiento respecto a las macros.

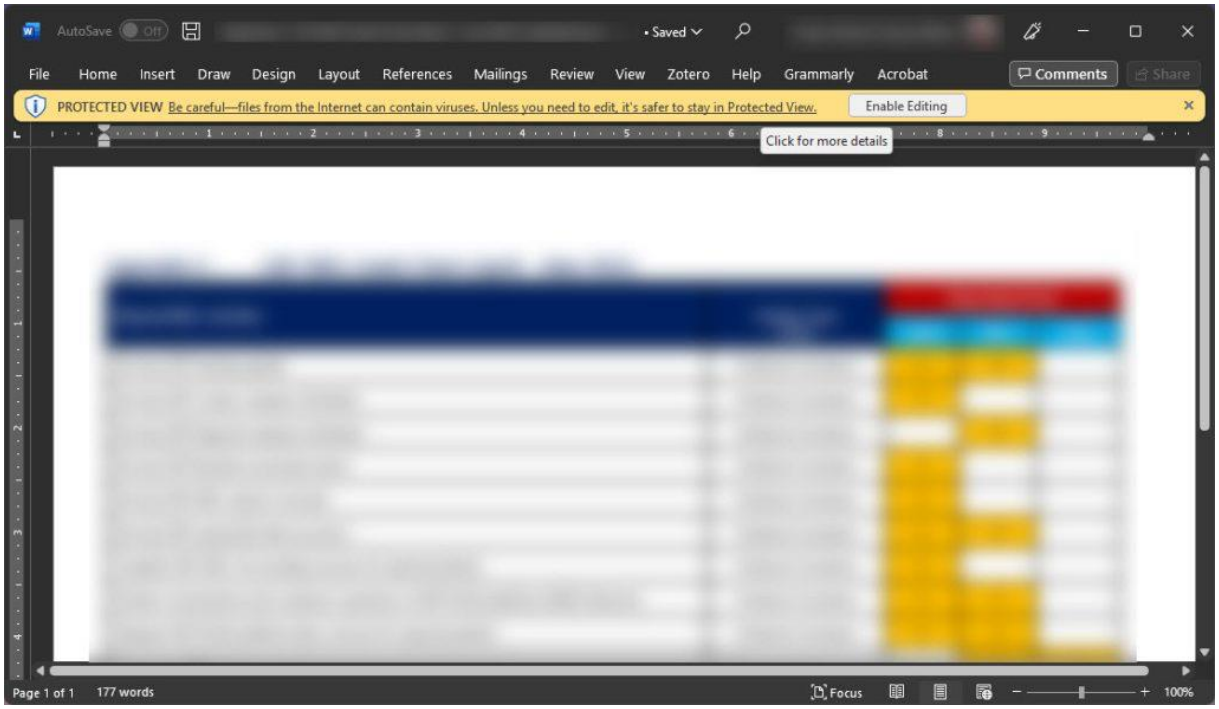


Centro de Confianza para MS Office (agosto de 2022, Menú Archivo->Opciones->Centro de Confianza->Configuración del Centro de Confianza->Configuración de macros)

Otra característica interesante de MS Office es la Vista protegida, que según el origen de un archivo, lo abre en un entorno aislado con pocos privilegios o acceso para interferir en la computadora, ofreciendo otra capa de confianza. Uno de los problemas con este modo es que, al igual que ocurre con el bloqueo de macros, hay un botón en una banda encima del documento en el que el usuario puede desactivar la función Vista protegida, lo que de nuevo permite ataques en los que el creador del documento engaña al usuario para que desactive esta protección.



Configuración de la Vista Protegida (agosto de 2022, Menú Archivo->Opciones->Centro de Confianza->Configuración del Centro de Confianza->Vista Protegida)



Vista protegida de un documento de MS Word (agosto de 2022)

Y ahora, ¿qué sigue?

Primero, cuando reciba un archivo sospechoso, usted tendrá la habilidad de ejecutar un primer análisis para detectar cualquier problema de seguridad evidente. Los escenarios potenciales pueden resumirse en éstos:

1. Si el archivo no parece contener nada dañino, podemos reducir el nivel de sospecha del archivo.
    - Si, por algún motivo, el objetivo tiene un alto nivel de riesgo, deberíamos volver a verificarlo con otros colegas o grupos más especializados.
2. Si el archivo parece malicioso, podríamos intentar buscar su hash en plataformas como VirusTotal. Si se trata de una muestra de malware conocida, encontraremos mucha información más detallada que nos será útil para comprender la naturaleza de la amenaza, la magnitud de la campaña, etc.
3. Si las amenazas contenidas en el archivo son fáciles de detectar y comprender, pero no son conocidas por la comunidad, deberíamos ser capaces de aportar alguna información específica al investigar más o buscar ayuda.
4. Si los elementos contenidos en el archivo parecen avanzados, difíciles de comprender o incluso complicados de categorizar como amenazas; y el hash del archivo es desconocido para las plataformas públicas, vale la pena contactarse con organizaciones más especializadas que puedan analizar mejor los archivos en busca de amenazas poco evidentes.

Además, en general recomendamos:

- Evitar ejecutar cualquier código sospechoso (a menos que comprenda los riesgos y tome las precauciones respectivas, las cuales no se abordan en este material).
- Investigar más sobre cualquier elemento específico que encuentre y desconozca. Hay muchos comandos y formas diferentes de lograr cosas con código, y es insostenible conocerlos todos, por lo que es normal y esperable revisar la documentación para buscar instrucciones o características específicas que le permitan comprender mejor la funcionalidad de una macro u otros objetos desconocidos.

Recuerde que el análisis de documentos maliciosos (y de malware en general) es una carrera completa que usualmente requiere años de experiencia para manejar casos más avanzados. Dicho esto, reforzamos que este material es una introducción a una parte específica del análisis de malware que esperamos anime al lector a aprender más y adquirir más habilidades en este campo. Sin embargo, dado el riesgo asociado a operar artefactos maliciosos sin los procesos y consideraciones de seguridad adecuados, desaconsejamos a los lectores agregar más procesos y herramientas de análisis a los flujos de trabajo presentados sin el conocimiento adecuado de dichos procesos y herramientas, especialmente aquellos que implican la ejecución de malware (o análisis dinámicos).

Este es un material en constante revisión. Para cualquier pregunta o comentario, por favor, contáctese con cguerra@internews.org