I. DATOS GENERALES:

Clase de alerta: Código malicioso

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Bajo

II. ALERTA

Investigadores del CERT de Japón han alertado de una nueva técnica que consiste en insertar un archivo malicioso de Microsoft Word dentro de un archivo PDF. Esta técnica ha sido bautizada como MalDoc en PDF.

Figura 1.- Tecnica MalDoc en PDF.

III. INTRODUCCIÓN

El equipo de respuesta a emergencias informáticas de Japón (JPCERT) está compartiendo detalles de un nuevo ataque 'MalDoc en PDF' detectado en julio de 2023 que evita la detección o confundir a las herramientas de análisis.

El ataque MalDoc, se basa en la creación de archivos conocidos como “políglotas”, que contienen dos formatos de archivo distintos en uno solo, estos archivos pueden parecer inofensivos en un formato conocido, pero esconden código malicioso en el otro. Por ejemplo, los documentos maliciosos en esta campaña son una combinación de documentos PDF y Word, para evadir la detección.

Los investigadores indican que un archivo creado con MalDoc en PDF puede abrirse a pesar de tener la estructura y los números mágicos propios de un archivo PDF; si el archivo está configurado con una macro, al abrirlo en Word, se ejecutará un script VBS (Visual Basic Script Edition) que realizará acciones perjudiciales.

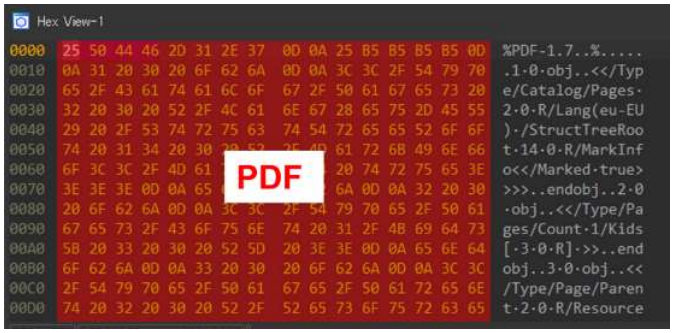
IV. VECTOR DE ATAQUE:

El archivo analizado por JPCERT es reconocido por la mayoría de los motores y herramientas de escaneo como PDF, pero las aplicaciones de oficina pueden abrirlo como un documento de Word normal (.doc).

La técnica implica la inserción de un archivo MHT[1] creado en Word, con una macro adjunta, dentro de un archivo PDF. El archivo resultante es un PDF válido que también puede abrirse en Microsoft Word. Si se abre como un archivo .DOC en Microsoft Office, el documento PDF incrustado en su interior activa una macro VBS diseñada para descargar e instalar un archivo de malware MSI si se abre como un archivo .doc en Microsoft Office.

A continuación, el siguiente documento PDF contiene un documento de Word con una macro VBS para descargar e instalar un archivo de malware MSI.

Al analizar un archivo creado con MalDoc en PDF, existe una alta posibilidad de que las herramientas de análisis de PDF no puedan detectar sus partes maliciosas, como se muestra en la Figura 2. Volcado del archivo malicioso



[1]Un archivo .MHT es un archivo MIME HTML Archive. Los archivos MHT se asocian comúnmente con el navegador web Internet Explorer; contienen archivos de páginas web guardados por un usuario mientras navega por Internet. Esta es una forma de almacenar una copia local de una página web. Los archivos MHT contienen una copia del código HTML, imágenes, iconos, estilos, etc. de una página web, en un único archivo que los usuarios pueden ver sin conexión.

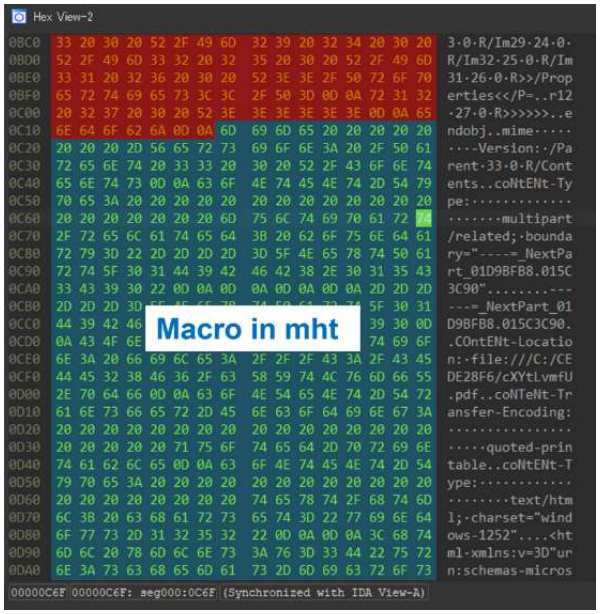


Figura 2.- ***Volcado del archivo malicioso***
Fuente: JPCERT

.

Se debe tener en cuenta que el archivo analizado, realiza comportamientos no intencionales cuando se abre en Word, mientras que los comportamientos maliciosos no se pueden confirmar cuando se abre en los visores de PDF; además, dado que el archivo se reconoce como un archivo PDF, el software sandbox o antivirus existente puede no detectarlo.

V. INDICADORES DE COMPROMISO

Referencias

[1] pdfid.py
https://github.com/DidierStevens/DidierStevensSuite/blob/master/pdfid.py

[2] OLEVBA
https://github.com/decalage2/oletools/wiki/olevba

Apéndice A: información de C2

- https [:] // cloudmetricsapp [.] com
- https [:] // web365metrics [.] com

Apéndice B: valor hash de malware

- ef59d7038cfd565fd65bae1258810d5361df938244ebad33b71882dcf683058
- 098796e1b82c199ad226bff056b6310262b132f6d06930d3c254c57bdf548187
- 5b677d297fb862c2d223973697479ee53a91d03073b14556f421b3d74f136b9d

VI. RECOMENDACIONES:

- La técnica utilizada por MalDoc en PDF descrita, no omite la configuración del Office que deshabilita la ejecución automática en la macro de Word. Por lo que, el EcuCERT recomienda a su comunidad objetivo deshabilitar la ejecución automática de macros en Microsoft Office en la pestaña Archivo/Opciones/ Centro de confianza > Configuración de Centro de Confianza/ Configuración de macro.

- Si se realiza un análisis de malware utilizando herramientas de sandbox para proteger su estación de trabajo.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

Masubuchi, Y. (28 de Agosto de 2023). *JPCERT / CC*. Obtenido de https://blogs.jpcert.or.jp/en/2023/08/maldocinpdf.html

MyR. (2023). *Opensecurity*. Obtenido de https://www.opensecurity.es/maldoc-en-pdf-y-otras-tecnicas-de-ingenieria-social/

Toulas, B. (28 de 08 de 2023). *BleepingComputer*. Obtenido de https://www.bleepingcomputer.com/news/security/maldoc-in-pdfs-hiding-malicious-word-docs-in-pdf-files/