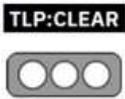


Nro. Alerta:	AL-2023-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	20-sep-2023	Ataque MalDoc en PDF	Pág.: 1 of 5

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.

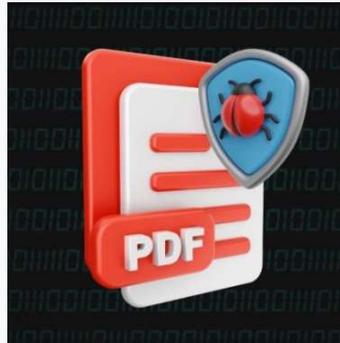
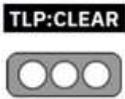


Figura 1.- Tecnica MalDoc en PDF.

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.

Nro. Alerta:	AL-2023-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	20-sep-2023	Ataque MalDoc en PDF	Pág.: 2 of 5

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).

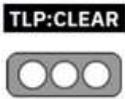
La técnica implica la inserción de un archivo MHT¹ creado en Word, con una macro adjunta, dentro de un archivo PDF. El archivo resultante es un PDF válido que también puede abrirse en Microsoft Word. Si se abre como un archivo .DOC en Microsoft Office, el documento PDF incrustado en su interior activa 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



¹Un 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.

Nro. Alerta:	AL-2023-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	20-sep-2023	Ataque MalDoc en PDF	V 1.1 Pág.: 3 of 5



```

Hex View-2
0BC0 33 20 30 20 52 2F 49 6D 32 39 20 32 34 20 30 20 30 0-R/Im29-24-0-
0BD0 52 2F 49 6D 33 32 20 32 35 20 30 20 52 2F 49 6D R/Im32-25-0-R/Im
0BE0 33 31 20 32 36 20 30 20 52 3E 3E 2F 50 72 6F 70 31-26-0-R>>/Prop
0BF0 65 72 74 69 65 73 3C 3C 2F 50 30 00 0A 72 31 32 erties<</P>...r12
0C00 20 32 37 20 30 20 52 3E 3E 3E 3E 3E 00 0A 65 -27-0-R>>>>>>...e
0C10 6E 64 6F 62 6A 00 0A 6D 69 6D 65 20 20 20 20 20 ndobj...mime....
0C20 20 20 20 20 56 65 72 73 69 6F 6E 3A 20 2F 50 61 ...Version:./Pa
0C30 72 65 6E 74 20 33 33 20 30 20 52 2F 43 6F 6E 74 rent-33-0-R/Cont
0C40 65 6E 74 73 00 0A 63 6F 4E 74 45 4E 74 2D 54 79 ents...coltEnt-Ty
0C50 70 65 3A 20 20 20 20 20 20 20 20 20 20 20 20 20 pe:.....
0C60 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....multipart
0C70 2F 72 65 6C 61 74 65 64 38 20 62 6F 75 6E 64 61 /related; bounda
0C80 72 79 30 22 20 20 20 20 30 5F 4E 65 78 74 50 61 ry="-----_NextPa
0C90 72 74 5F 30 31 44 39 42 46 42 38 2E 30 31 35 43 rt_01D9BF88_015C
0CA0 33 43 39 30 22 00 0A 00 0A 00 0A 00 0A 20 2D 2D 3C90".....
0CB0 20 2D 2D 3D 5F 4E 65 78 74 65 64 33 74 5F 30 31 ----_NextPart_01
0CC0 44 39 42 46 00 00 00 00 00 00 00 00 00 00 00 D9BF88_015C3C90.
0CD0 0A 43 4F 6E 74 69 6F 74 69 6F 74 69 6F .Content-Locatio
0CE0 6E 3A 20 66 69 6C 65 3A 2F 2F 2F 43 3A 2F 43 45 n:-file:///C:/CE
0CF0 44 45 32 38 46 36 2F 63 58 59 74 4C 76 6D 66 55 DE28F6/cXyLvmfU
0D00 2E 70 64 66 00 0A 63 6F 4E 54 65 4E 74 2D 54 72 .pdf...coltEnt-Tr
0D10 61 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A ansfer-Encoding:
0D20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
0D30 20 20 20 20 20 71 75 6F 74 65 64 2D 70 72 69 6E .....quoted-prin
0D40 74 61 62 6C 65 00 0A 63 6F 4E 74 45 4E 74 2D 54 table...coltEnt-T
0D50 79 70 65 3A 20 20 20 20 20 20 20 20 20 20 20 20 20 ype:.....
0D60 20 20 20 20 20 20 20 20 20 74 65 78 74 2F 68 74 6D .....text/htm
0D70 6C 38 20 63 68 61 72 73 65 74 3D 22 77 69 6E 64 l;.charset="wind
0D80 6F 77 73 2D 31 32 35 32 22 00 0A 00 0A 3C 68 74 ows-1252"....<ht
0D90 6D 6C 20 78 6D 6C 6E 73 3A 76 3D 33 44 22 75 72 ml+xmlns:v=3D"ur
0DA0 6E 3A 73 63 68 65 6D 61 73 2D 6D 69 63 72 6F 73 n:schemas-micros
00000C6F 00000C6F: _seg00:0C6F (Synchronized with IDA View-A)
  
```

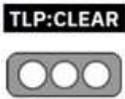
Figura 2.- Volcado del archivo malicioso
 Fuente: JPCERT

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>

Nro. Alerta:	AL-2023-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	20-sep-2023	Ataque MalDoc en PDF	Pág.: 4 of 5

Apéndice A: información de C2

- [https \[: \] // cloudmetricsapp \[. \] com](https://cloudmetricsapp.com)
- [https \[: \] // web365metrics \[. \] 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>

Nro. Alerta:	AL-2023-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	
TLP:			V 1.1
Fecha:	20-sep-2023	Ataque MalDoc en PDF	Pág.: 5 of 5

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/>