Los expertos en ciberseguridad han señalado una novedosa técnica de evasión de antivirus que implica la inserción de un archivo malicioso de Microsoft Word en un archivo PDF.

Este astuto método, bautizado como «MalDoc in PDF» por JPCERT/CC, se dice que se utilizó en un ataque en el entorno real en julio de 2023.

> Los investigadores Yuma Masubuchi y Kota Kino afirmaron: *«Un archivo creado con MalDoc in PDF puede abrirse en Word a pesar de que posee los números mágicos y la estructura de archivo de un PDF». «Si el archivo contiene una macro configurada, al abrirlo en Word, se ejecuta VBS y lleva a cabo comportamientos maliciosos».*

Estos archivos especialmente diseñados son conocidos como «*políglotas*«, ya que constituyen una forma legítima de varios tipos de archivos diferentes, en este caso, tanto PDF como Word (DOC).

Esto implica la adición de un archivo MHT creado en Word y con una macro adjunta después del objeto de archivo PDF. El resultado final es un archivo PDF válido que también puede abrirse en la aplicación Word.

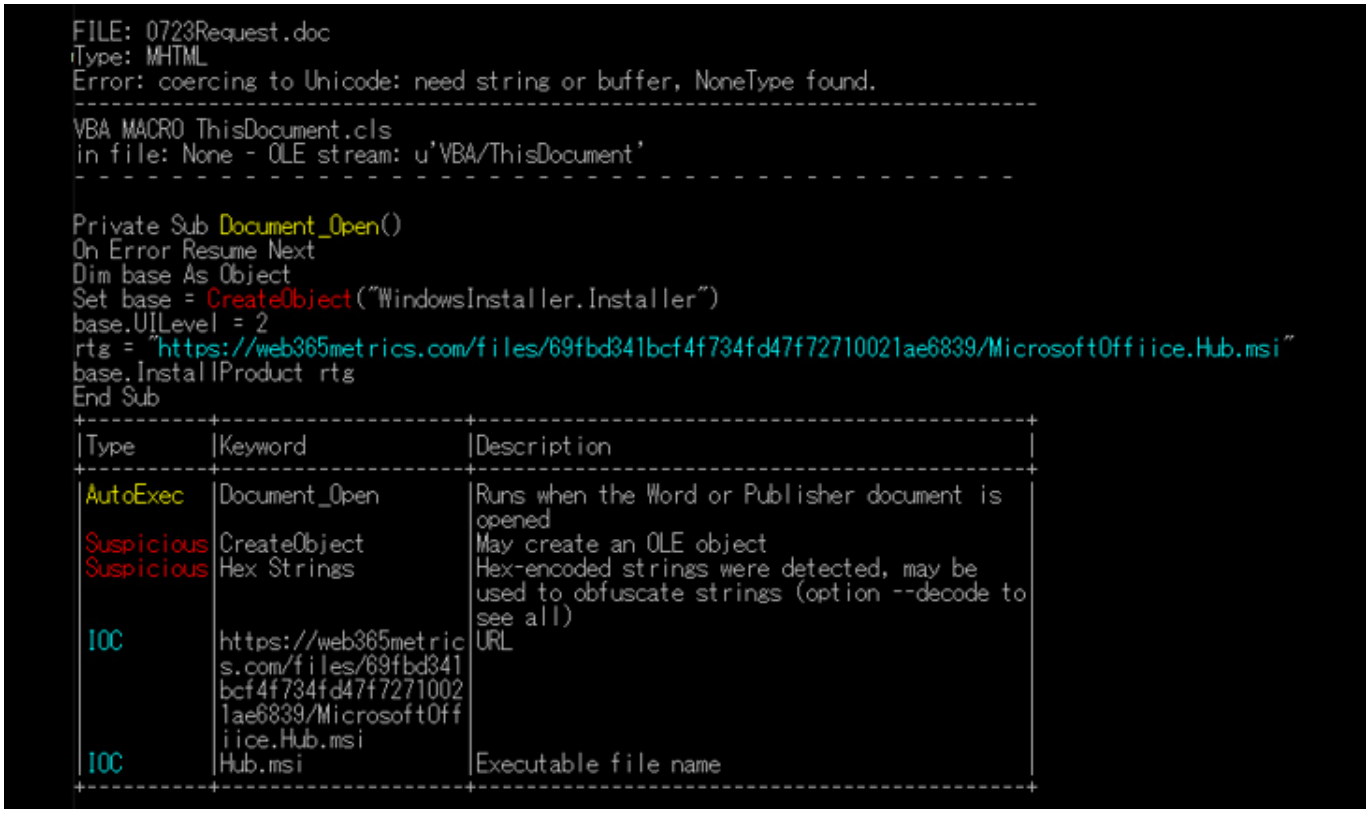
Dicho de otra manera, el documento PDF se incorpora a sí mismo como un documento de Word con una macro VBS diseñada para descargar e instalar un archivo de malware MSI si se abre como un archivo .DOC en Microsoft Office. No está claro de inmediato qué tipo de malware se distribuyó de esta manera.

> Will Dormann, investigador de seguridad, afirmó: *«Cuando se descarga un documento de Internet o se recibe por correo electrónico, llevará un 'MotW'. Como resultado, el usuario deberá hacer clic en 'Habilitar edición' para salir del Modo Protegido. En ese momento, se dará cuenta de que las macros están desactivadas».*

Aunque los ataques del mundo real que utilizan MalDoc in PDF se observaron hace un poco más de un mes, existen pruebas que sugieren que se estaba experimentando con esta técnica («DummymhtmldocmacroDoc.doc«) ya en mayo, según destacó Dormann.

Este desarrollo tiene lugar en medio de un aumento en las campañas de phishing que emplean códigos QR para propagar direcciones URL maliciosas, una técnica conocida como «*qishing*«.

> *«Las muestras que hemos detectado utilizando esta técnica se presentan principalmente como notificaciones de autenticación de múltiples factores (MFA), que atraen a sus víctimas para escanear el código QR con sus teléfonos móviles y obtener acceso»,* afirmó Trustwave la semana pasada.



> *«Sin embargo, en lugar de dirigirse a la ubicación deseada por la víctima, el código QR la redirige a la página de phishing del actor malicioso.»*

Una campaña de este tipo que apunta a las credenciales de Microsoft de los usuarios ha experimentado un aumento de más del 2,400% desde mayo de 2023, según señaló Cofense en agosto, destacando cómo *«escanear un código QR en un dispositivo móvil coloca al usuario fuera de las salvaguardias del entorno empresarial».*

Los ataques de ingeniería social, como se evidencian en los ataques asociados con LAPSUS$ y Muddled Libra, se vuelven más intrincados y avanzados a medida que los actores de amenazas aprovechan tácticas de voz (vishing) y de suplantación de identidad (phishing) para obtener acceso no autorizado a sistemas objetivo.

En una instancia resaltada por Sophos, un actor malicioso combinó señuelos telefónicos y de correo electrónico para ejecutar una cadena de ataques compleja contra un empleado de una organización con sede en Suiza.

> *«La persona que llamó, cuya voz parecía la de un hombre de mediana edad, le informó al empleado que era un conductor de entrega con un paquete urgente destinado a una de las ubicaciones de la empresa, pero que no había nadie disponible para recibirlo. Luego, solicitó una nueva dirección de entrega en la ubicación de la oficina del empleado»,* dijo el investigador de Sophos, Andrew Brandt.

> *«Para que se realice la nueva entrega del paquete, continuó explicando, el empleado tendría que leer en voz alta un código que la empresa de envíos enviaría por correo electrónico».*

El correo electrónico supuestamente enviado por la empresa de envíos logró convencer a la víctima de abrir lo que parecía ser un archivo PDF que contenía el código. Sin embargo, en realidad resultó ser una imagen estática incrustada en el cuerpo del mensaje, diseñada para parecer *«exactamente como un mensaje de Outlook con un archivo adjunto de correo electrónico».*

El ataque de spam con imágenes falsas finalmente llevó al receptor a un sitio web fraudulento mediante una cadena de redireccionamiento que, a su vez, descargó un archivo ejecutable engañoso que se hacía pasar por un servicio de paquetería denominado *«Servicio de Paquetes Universales»*. Cuando se ejecutó, actuó como un conducto para entregar scripts adicionales de PowerShell destinados a robar datos y enviar señales a un servicio oculto de TOR remoto.

En otra campaña destacada por Cyble, se descubrió que un Script de Visual Basic ejecutado a través de un archivo de Microsoft Excel malicioso empleaba código PowerShell para descargar una imagen JPG que contenía una carga útil oculta en Base64 de .NET, como Agent Tesla, LimeRAT y Remcos RAT, desde un servidor remoto.

Estos acontecimientos también coinciden con preocupaciones en materia de seguridad relacionadas con colisiones de nombres en el Sistema de Nombres de Dominio (DNS) que podrían ser explotadas para filtrar información confidencial.

> *«Las colisiones de nombres no son la única situación que puede causar que un dominio de nivel superior se comporte de manera inusual. Algunos no responden adecuadamente cuando se les presentan nombres que han caducado o que nunca han existido»*, señaló Cisco Talos en un artículo reciente.

> *«En estos TLD, los nombres de dominio no registrados y caducados todavía resuelven a direcciones IP. Algunos de estos TLD incluso publican registros MX y recopilan correos electrónicos para los nombres en cuestión».*