En noviembre del año pasado, ESET detectó una campaña de malware que involucra restaurantes de comida rápida, bancos y demás empresas, y que además utiliza los anuncios de Facebook para propagarse.

Se trata del troyano bancario Mispadu, que actualmente está funcionando en Latinoamérica.

Este troyano se ha identificado en campañas dirigidas a Brasil y México. Está escrito en Delphi. Debido a que funciona como puerta trasera, Mispadu puede tomar capturas de pantalla, simular acciones de mouse y teclado, capturar las pulsaciones de las teclas y se actualiza a través de un archivo de Visual Basic Script (VBS) que descarga y ejecuta.

Al igual que otras piezas de malware como Amavaldo y Casbaneiro, Mispadu puede identificarse mediante el uso de un algoritmo criptográfico único y personalizado, para ofuscar las cadenas en su código.

Ahora, en junio de 2020, se ha popularizado una campaña publicitaria en Facebook que muestra anuncios con cupones de descuento de McDonalds, como se puede ver en la siguiente imagen:

Aunque para muchos es fácil darse cuenta que es un anuncio falso, por el hecho de que no aparece el check de verificación al lado del nombre de la fanpage al colocar el cursor, y que el dominio no es el correcto, muchas personas podrían caer en la trampa por la atractiva promoción de pagar 19 pesos por una hamburguesa.

Al dar clic en el botón Más información, se abre una página cuyo dominio cambia a cupon[.]mcdonalds[.]tech. Según los datos de Who.is, el sitio web está creado con Wix, y es una copia idéntica del sitio web original de McDonalds.

Si se da clic en generar cupón, se descarga un archivo zip con el nombre Cupón-18002.zip, el

cual contiene un archivo MSI y otros dos archivos ejecutables de Windows.

Podría tratarse de una variante del troyano Mispadu, ya que hasta ahora, el archivo ZIP no es detectado por ningún antivirus. Sin embargo, VirusTotal detecta a uno de los archivos con una gran variedad de nombres vistos en la naturaleza, por ejemplo, cvr8bff.tmp.cvr. y que es un producto creado por Mozilla y firmado por la misma compañía y Symantec.

ESET no detecta el malware, probablemente porque el algoritmo SHA1 es distinto al detectado en la campaña del año pasado, lo que sugiere un nuevo método de ofuscación.

Es evidente que Facebook no se preocupa por el contenido que muestra en su plataforma, mismo por el cual recibe una remuneración.

Hemos contactado a McDonald’s México para saber si están al tanto de esta campaña de malware que involucra su nombre desde hace varios meses y si le interesa emitir algún comunicado al respecto, en caso de recibir respuesta se actualizará esta nota.

Debido al algoritmo de Facebook para mostrar anuncios relevantes, nos apareció un anuncio auténtico de McDonald’s, que se ve así:

En este anuncio auténtico, se puede observar que el dominio del sitio web es el correcto, además, al poner el cursor sobre el nombre McDonald’s de la fanpage, aparece el check de página verificada.

Como el restaurante está emitiendo anuncios con promociones, es muy probable que la gente se confunda y accedan al sitio equivocado, infectándose con el malware. Es necesario tener mucho cuidado en este aspecto y verificar siempre que el dominio del sitio sea el correcto y que la página en Facebook sea la auténtica.