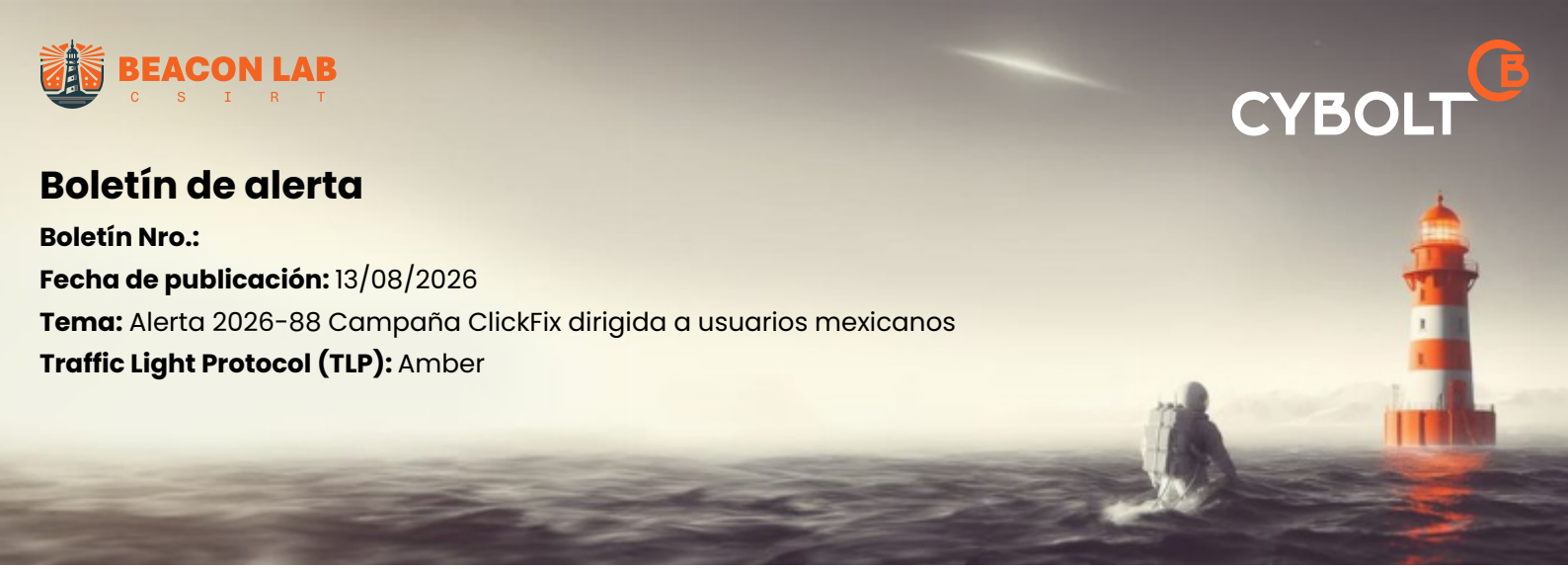


Boletín de alerta

Boletín Nro.:
Fecha de publicación: 13/08/2026
Tema: Alerta 2026-88 Campaña ClickFix dirigida a usuarios mexicanos
Traffic Light Protocol (TLP): Amber

Descripción

Se ha identificado una campaña de **phishing e ingeniería social** dirigida a usuarios en México que utiliza como señuelo un supuesto **"comprobante de pago"** y documentación que aparenta estar relacionada con el **Servicio de Administración Tributaria (SAT)**.

De acuerdo con el flujo observado y la información proporcionada para este boletín, la víctima recibe un correo electrónico proveniente de una **dirección externa perteneciente al dominio Gmail**, utilizando el asunto:

"comprobante de pago"

El mensaje contiene como archivo adjunto un **documento PDF protegido**, diseñado para aparentar ser documentación legítima relacionada con el SAT.

La protección del PDF, la temática fiscal y la apariencia institucional del documento buscan incrementar la credibilidad del mensaje y generar suficiente confianza para que la víctima continúe con las instrucciones presentadas.

Al interactuar con el contenido o con el mecanismo incluido en el documento, la víctima es conducida a la siguiente etapa del ataque, donde comienza una cadena de ingeniería social conocida como **ClickFix**.

A diferencia de ataques tradicionales que explotan directamente una vulnerabilidad técnica del sistema operativo, **ClickFix utiliza al propio usuario para ejecutar las instrucciones maliciosas**.

ClickFix es una técnica de ingeniería social mediante la cual los atacantes manipulan a los usuarios para que ejecuten manualmente comandos maliciosos en su propio sistema.

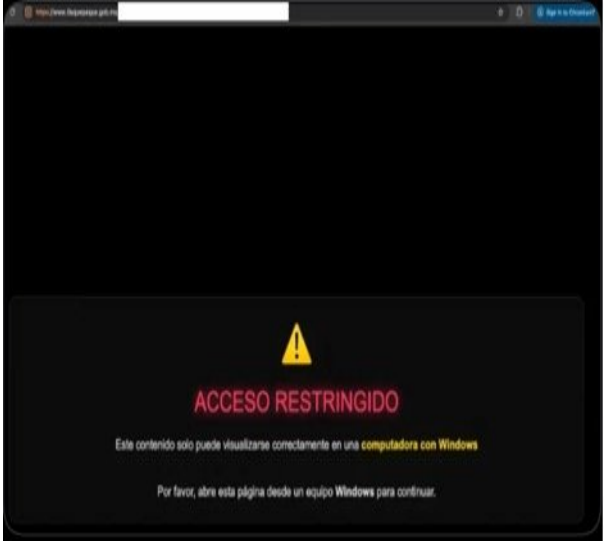
Campañas ClickFix documentadas públicamente han sido utilizadas para distribuir malware como **Lumma Stealer, Latrodectus, NetSupport RAT y DarkGate**, demostrando que esta técnica funciona principalmente como un mecanismo de entrega y ejecución inicial; el payload final puede variar dependiendo del atacante.

Todo inicia con un correo como este «Comprobante de pago», supuestamente del SAT.

Cuando el usuario descarga y abre el archivo adjunto en PDF, obliga al usuario a dar clic en el botón «Desbloquear»

Cuando el usuario da clic, es enviado a la página del Gobierno de Tlaquepaque y ahí se explota una vulnerabilidad automáticamente. Esta vulnerabilidad vuelve a enviar al usuario a otrá página comprometida por el atacante. Esta página no es del gobierno, pero si es un sitio mexicano. En esa página, se ejecuta otro “programa”, lo que ven en la imágen es el código del programa. Este programa funciona como un policía, antes de pasar al segundo paso, hace una revisión.

Primero analiza si la víctima es un programa como un antivirus o programas que existen en internet que puedan detectar este tipo de amenazas. – Después valida si la víctima usa Windows, sino usa Windows, le muestra esta pantalla. Lo que nos indica que este ataque solo funciona para usuarios de Windows. Si es MacOS por ejemplo, les muestra esta pantalla y termina el ataque.



Si la computadora de la víctima es Windows, detecta la dirección IP de la víctima y la envía a los atacantes, si la IP es de México, envía el mensaje: « *WINDOWS REAL* — Objetivo premium». También envía al atacante la zona horaria de la computadora. De acuerdo al mensaje y el código del mensaje que envía, podemos determinar que el atacante utilizan Telegram o Whatsapp para recibir estos mensajes. en ubicaciones arbitrarias del sistema host utilizando los privilegios del usuario o proceso que ejecutó docker cp.

Solución

Los usuarios y administradores deben realizar las siguientes acciones:

- No abrir archivos PDF inesperados relacionados con supuestos comprobantes de pago.
- Desconfiar de correos provenientes de cuentas externas que pretendan representar al SAT.
- Validar cualquier comunicación fiscal directamente mediante los portales oficiales del SAT.
- No ejecutar instrucciones que soliciten utilizar Windows + R.
- No pegar comandos proporcionados por sitios web desconocidos en PowerShell, CMD o Windows Terminal.

Información adicional:

- **Publicación original compartida en X – @hiramcoop**
- **Microsoft Threat Intelligence – Think before you Click(Fix): Analyzing the ClickFix social engineering technique**
- **Palo Alto Networks Unit 42 – Fix the Click: Preventing the ClickFix Attack Vector**
- **R3D – Campañas de phishing que suplantan al SAT mediante documentos PDF**