Microsoft ha revelado detalles sobre una campaña de phishing en curso dirigida al sector hotelero, en la que los atacantes se hacen pasar por la agencia de viajes en línea Booking.com. Para ello, utilizan una técnica de ingeniería social cada vez más común llamada *ClickFix*, diseñada para distribuir malware que roba credenciales.

Según el equipo de inteligencia de amenazas de Microsoft, esta actividad comenzó en diciembre de 2024 con el objetivo de llevar a cabo fraudes financieros y robos. La compañía ha identificado la campaña bajo el nombre *Storm-1865*.

> *«Este ataque de phishing se dirige específicamente a empleados de organizaciones hoteleras en América del Norte, Oceanía, Asia del Sur y el Sudeste Asiático, así como en diversas regiones de Europa. Dado que estos profesionales suelen interactuar con Booking.com, los atacantes les envían correos electrónicos falsificados que parecen provenir de la agencia»*, explicó Microsoft en un informe compartido con *The Hacker News*.

La técnica *ClickFix* y su método de engaño

La técnica *ClickFix* ha ganado popularidad en los últimos meses porque engaña a los usuarios para que ejecuten malware bajo el pretexto de corregir un supuesto error inexistente. Para ello, los atacantes proporcionan instrucciones que la víctima debe copiar, pegar y ejecutar, iniciando así la infección. Este método se detectó por primera vez en octubre de 2023.

El ataque comienza con *Storm-1865* enviando un correo malicioso a la víctima, notificándole sobre una supuesta reseña negativa publicada por un «huésped» en Booking.com. En el mensaje se solicita al destinatario que brinde su opinión, incluyendo un enlace o un archivo PDF con un enlace que, en apariencia, dirige al sitio de reservas.

Sin embargo, al hacer clic, el usuario es redirigido a una página falsa de verificación CAPTCHA, diseñada para parecerse a una página legítima de Booking.com. Esta táctica genera una falsa sensación de seguridad y aumenta la probabilidad de éxito del ataque.

> *«El CAPTCHA falso es el punto donde la técnica ClickFix entra en juego para descargar el malware. El sitio web instruye al usuario para que use un atajo de teclado que abre la ventana Ejecutar de Windows, luego copia y ejecuta un comando que el sitio agrega al portapapeles»,* explicó Microsoft.

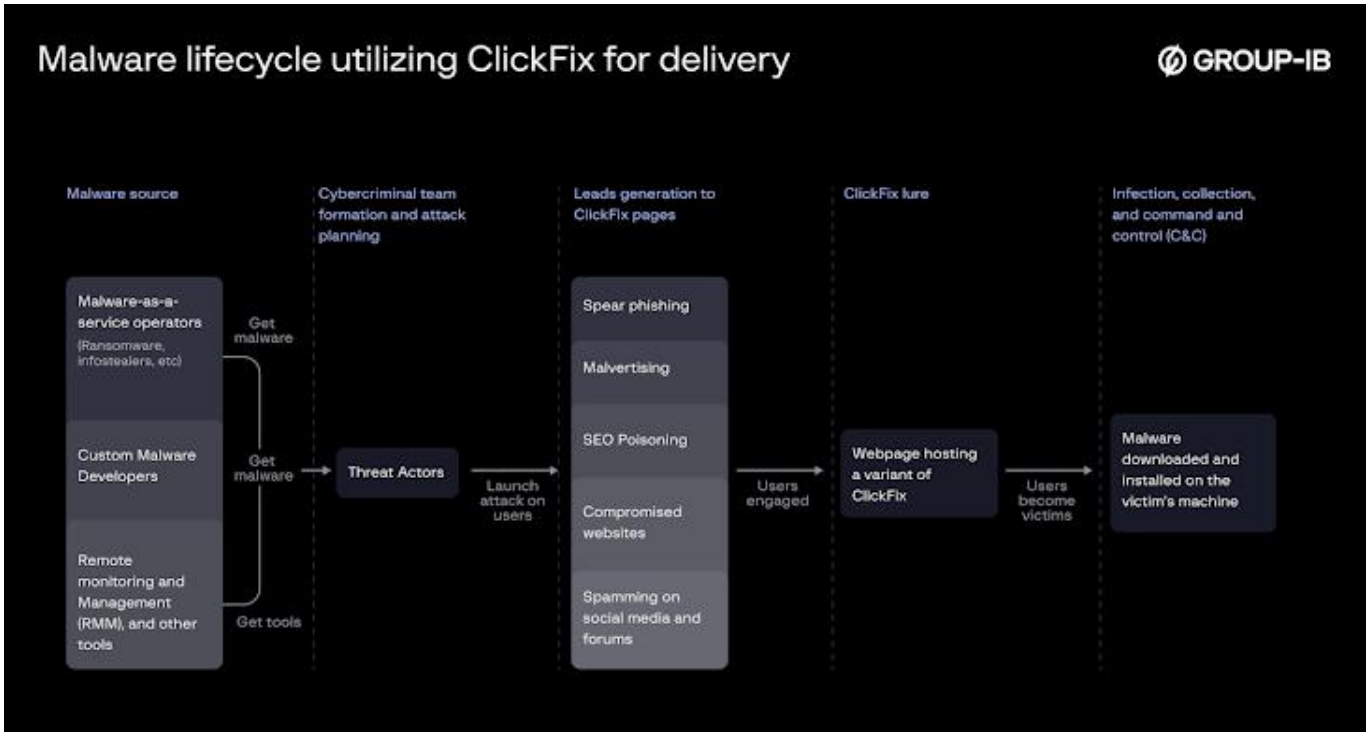
Este comando utiliza el binario legítimo *mshta.exe* para desplegar una segunda fase del ataque, introduciendo diferentes tipos de malware, entre ellos *XWorm, Lumma Stealer, VenomRAT, AsyncRAT, Danabot* y *NetSupport RAT*.

Una evolución en las tácticas de ataque

Microsoft también señaló que *Storm-1865* ha llevado a cabo campañas previas dirigidas a compradores en plataformas de comercio electrónico, utilizando correos de phishing para redirigirlos a sitios de pago fraudulentos. La incorporación de *ClickFix* a estas tácticas representa una evolución en su enfoque, diseñada para evadir las medidas de seguridad tradicionales contra phishing y malware.

> *«El actor de amenazas identificado como Storm-1865 ejecuta campañas de phishing para robar datos de pago y realizar cargos fraudulentos. Desde principios de 2023, estas campañas han ido en aumento y utilizan plataformas de terceros como agencias de viajes en línea, servicios de comercio electrónico y proveedores de correo como Gmail e iCloud Mail»,* indicó Microsoft.

La combinación de señuelos relacionados con Booking.com y la técnica *ClickFix* para propagar *XWorm* también ha sido documentada por la firma de ciberseguridad *Cofense*, que destacó que este método se utilizó casi el doble de veces con *XWorm RAT* en comparación con otras familias de malware.



Storm-1865 no es la única campaña que ha adoptado *ClickFix* como método de distribución de malware. La técnica ha demostrado ser tan efectiva que incluso grupos de ciberespionaje estatales de Rusia e Irán, como *APT28* y *MuddyWater*, la han implementado para engañar a sus víctimas.

> *«El método explota el comportamiento humano: al presentar una 'solución' creíble para un problema aparente, los atacantes trasladan la ejecución del malware a la propia víctima, eludiendo muchas defensas automatizadas»*, explicó la firma *Group-IB* en un informe independiente publicado el viernes.

Una de las campañas documentadas por esta empresa de ciberseguridad muestra el uso de *ClickFix* para desplegar un descargador llamado *SMOKESABER*, que luego instala *Lumma Stealer*. Otros ataques han utilizado técnicas como publicidad maliciosa (*malvertising*), manipulación de motores de búsqueda (*SEO poisoning*), abuso de problemas en GitHub y la

publicación de enlaces a páginas *ClickFix* en foros y redes sociales.

Expansión del uso de *ClickFix* en el cibercrimen

Según *Group-IB*, el auge de *ClickFix* refleja una evolución en las estrategias de ingeniería social, aprovechando la confianza del usuario y las funciones del navegador para distribuir malware con facilidad. Su rápida adopción por parte de ciberdelincuentes y grupos de amenazas avanzadas persistentes (APT) demuestra su efectividad y la baja barrera técnica para su implementación.

Algunas de las campañas recientes que han utilizado *ClickFix* incluyen:

- Uso de CAPTCHAs falsos para iniciar un proceso de ejecución en múltiples etapas con *PowerShell*, entregando *Lumma* y *Vidar Stealer*.
- Uso de retos de *Google reCAPTCHA* falsificados por el grupo *Blind Eagle* para distribuir malware.
- Uso de enlaces falsos de confirmación de reservas para redirigir a las víctimas a páginas de verificación CAPTCHA que instalan *Lumma Stealer*.
- Uso de sitios web falsificados con apariencia de Windows para redirigir a las víctimas a páginas de CAPTCHA fraudulentas que descargan *Lumma Stealer*.

Además, otra campaña detectada recientemente ha demostrado la versatilidad del *Lumma Stealer*, distribuyéndolo a través de repositorios falsos en GitHub con contenido generado por inteligencia artificial (IA), utilizando un cargador denominado *SmartLoader*.

Estos repositorios maliciosos se camuflan como herramientas inofensivas, incluyendo trucos para videojuegos, software pirateado y utilidades de criptomonedas, según un análisis publicado a principios de esta semana por Trend Micro. *«La campaña atrae a las víctimas con la promesa de funciones gratuitas o no autorizadas, incitándolas a descargar archivos ZIP (por ejemplo, Release.zip, Software.zip)».*

Esta operación pone en evidencia cómo los ciberdelincuentes están aprovechando la

confianza en plataformas populares como GitHub para propagar malware.

Estos hallazgos coinciden con un informe de Trustwave sobre una campaña de phishing por correo electrónico que utiliza señuelos relacionados con facturas para distribuir una versión actualizada de StrelaStealer, un malware diseñado para el robo de información y presuntamente operado por un actor de amenazas identificado como Hive0145.

> *«Las muestras de StrelaStealer presentan múltiples capas de ofuscación personalizada y técnicas de alteración del flujo de código para dificultar su análisis. Se ha informado que el atacante podría haber desarrollado un 'crypter' especializado llamado 'Stellar loader', diseñado específicamente para usarse con StrelaStealer»*, explicó la compañía