Microsoft ha emitido una advertencia sobre varias campañas de phishing que utilizan temas relacionados con impuestos para distribuir malware y robar credenciales de acceso.

Según un informe, estas campañas emplean métodos de redirección como acortadores de URL y códigos QR incrustados en archivos adjuntos maliciosos. Además, abusan de servicios legítimos como plataformas de almacenamiento de archivos y páginas de perfil empresarial para evitar ser detectadas.

Un elemento destacado es que los usuarios son dirigidos a páginas falsas de inicio de sesión a través de una plataforma de *phishing como servicio* (PhaaS), identificada como RaccoonO365. Esta plataforma criminal fue detectada por primera vez en diciembre de 2024.

Entre las amenazas distribuidas se encuentran troyanos de acceso remoto (RATs) como *Remcos RAT*, así como otros tipos de malware y herramientas de post-explotación, incluidos *Latrodectus*, *AHKBot*, *GuLoader* y *BruteRatel C4 (BRc4)*.

Una de estas campañas fue observada por Microsoft el 6 de febrero de 2025, justo antes del inicio de la temporada de declaración de impuestos en EE.UU. Se estima que envió cientos de correos electrónicos con el objetivo de entregar *BRc4* y *Latrodectus*. Esta actividad se atribuye al grupo Storm-0249, conocido previamente por distribuir malware como *BazaLoader*, *IcedID*, *Bumblebee* y *Emotet*.

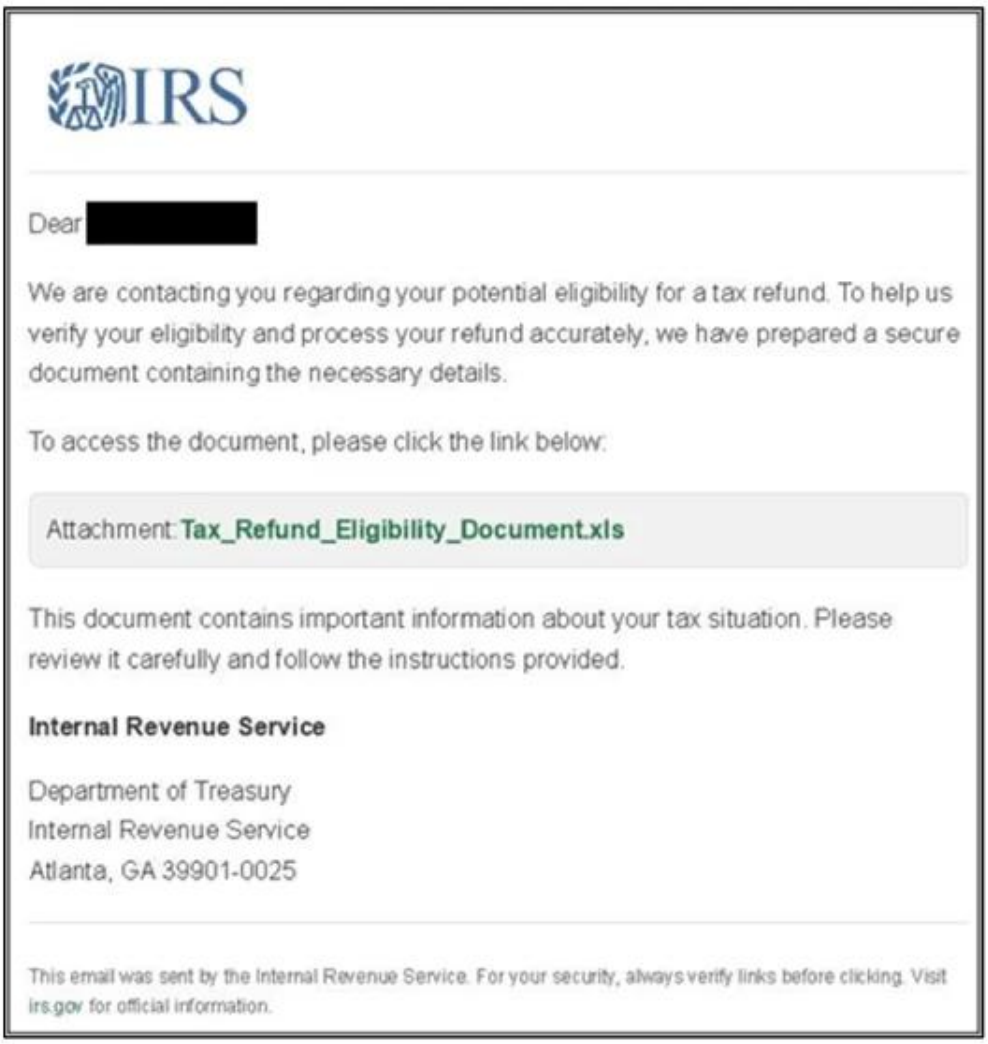
En los ataques, se usan archivos PDF con enlaces acortados mediante Rebrandly, los cuales redirigen a páginas falsas de Docusign. Al hacer clic en el botón de descarga, el resultado varía dependiendo de si el sistema del usuario cumple ciertos filtros definidos por los atacantes.

- Si se permite el acceso, se descarga un archivo JavaScript que a su vez obtiene un instalador MSI de Microsoft que distribuye *BRc4* y posteriormente *Latrodectus*.
- Si el usuario no es considerado un objetivo «valioso», se le entrega un PDF inofensivo desde el dominio royalegroupnyc[.]com.

Entre el 12 y el 28 de febrero de 2025, Microsoft también detectó una segunda campaña dirigida a más de 2,300 organizaciones estadounidenses, especialmente en los sectores de ingeniería, TI y consultoría. En este caso, los correos no contenían texto, pero sí un archivo PDF con un código QR que llevaba a una página falsa de inicio de sesión de Microsoft 365, gestionada también por RaccoonO365, para robar credenciales.

Estas campañas adoptan diversas formas y también han sido usadas para distribuir otros tipos de malware como *AHKBot* y *GuLoader*:

- AHKBot: lleva a los usuarios a un sitio donde se descarga un archivo de Excel malicioso. Al habilitar macros, se ejecuta un instalador MSI que lanza un script de AutoHotKey. Este script descarga un módulo que toma capturas de pantalla del equipo comprometido y las envía a un servidor remoto.
- GuLoader: engaña al usuario para que haga clic en un enlace dentro de un archivo PDF adjunto, lo que descarga un archivo ZIP con accesos directos (.lnk) disfrazados de documentos fiscales. Al ejecutarlos, se utiliza PowerShell para descargar un PDF y un archivo por lotes (.bat), que finalmente instala *Remcos*.


IRS

Dear [redacted]

We are contacting you regarding your potential eligibility for a tax refund. To help us verify your eligibility and process your refund accurately, we have prepared a secure document containing the necessary details.

To access the document, please click the link below:

Attachment: **Tax_Refund_Eligibility_Document.xls**

This document contains important information about your tax situation. Please review it carefully and follow the instructions provided.

Internal Revenue Service

Department of Treasury
Internal Revenue Service
Atlanta, GA 39901-0025

This email was sent by the Internal Revenue Service. For your security, always verify links before clicking. Visit irs.gov for official information.

Todo esto ocurre tras otra campaña de Storm-0249, en la que se redirigía a usuarios hacia sitios falsos que ofrecían supuestas descargas de *Windows 11 Pro*. Usaban la herramienta *BruteRatel* para distribuir una versión reciente del malware *Latrodectus*. Según Microsoft, el tráfico a estas páginas falsas probablemente fue generado a través de Facebook, ya que se detectaron URLs de referencia provenientes de esa red social.

La versión más reciente de *Latrodectus* (v1.9), detectada en febrero de 2025, incluye mejoras como tareas programadas para persistencia y la capacidad de ejecutar comandos de Windows mediante `cmd.exe`.

Este informe se suma a una creciente ola de ataques que utilizan códigos QR en documentos de phishing para ocultar URLs maliciosas, afectando tanto a Europa como a EE.UU. y provocando el robo masivo de credenciales.

Según un informe de Unit 42 de Palo Alto Networks, el análisis de las URLs extraídas de los códigos QR utilizados en estas campañas demuestra que los atacantes evitan incluir enlaces que dirijan directamente a dominios de phishing. En su lugar, prefieren usar mecanismos de redirección o aprovechar redirecciones abiertas en sitios legítimos para ocultar sus intenciones maliciosas.

Este hallazgo se suma a una serie de campañas recientes de phishing y técnicas de ingeniería social, entre las que destacan:

- El uso de la técnica «navegador dentro del navegador» (BitB) para mostrar ventanas emergentes falsas que imitan navegadores reales, engañando a jugadores de Counter-Strike 2 para que ingresen sus credenciales de Steam. El objetivo probable es revender el acceso a esas cuentas.
- El uso de malware tipo «stealer» para secuestrar cuentas de MailChimp, permitiendo a los atacantes enviar correos electrónicos masivos de forma fraudulenta.
- El uso de archivos SVG (gráficos vectoriales escalables) para eludir filtros antispam y redirigir a los usuarios a páginas falsas de inicio de sesión de Microsoft.
- El aprovechamiento de servicios de colaboración confiables como Adobe, DocuSign, Dropbox, Canva y Zoho, con el fin de evitar los filtros de seguridad de correos empresariales (SEGs) y robar credenciales.
- Campañas de phishing que suplantan plataformas de música en streaming, como Spotify y Apple Music, buscando recolectar credenciales y datos de pago de los usuarios.
- El despliegue de falsas alertas de seguridad sobre actividad sospechosa en dispositivos Windows o macOS, mostradas en sitios fraudulentos, para engañar a los usuarios y que entreguen sus credenciales del sistema.
- La distribución de instaladores de Windows falsificados para programas populares como DeepSeek, i4Tools y Youdao Dictionary Desktop, los cuales contienen el troyano

de acceso remoto Gh0st RAT.
- Envío de correos de phishing con temática de facturación dirigidos a empresas españolas, utilizados para propagar un malware robainformación conocido como DarkCloud.
- Suplantación de identidad de un banco rumano en correos electrónicos de phishing, con el objetivo de infectar organizaciones en Rumania con el malware Masslogger, también orientado al robo de información.

Recomendaciones para mitigar riesgos

Para protegerse ante estas amenazas, se recomienda que las organizaciones:

- Implementen métodos de autenticación resistentes al phishing (por ejemplo, claves de seguridad físicas o autenticación sin contraseña).
- Usen navegadores con protección contra sitios maliciosos.
- Activen controles de protección de red para evitar que los usuarios o aplicaciones accedan a dominios peligrosos.