Investigadores en ciberseguridad han identificado una masiva campaña de phishing que emplea imágenes falsas de CAPTCHA, distribuidas a través de documentos PDF alojados en la red de entrega de contenido (CDN) de Webflow, con el objetivo de propagar el malware Lumma Stealer.

Según Netskope Threat Labs, se han detectado 260 dominios únicos que albergan alrededor de 5,000 archivos PDF fraudulentos, los cuales redirigen a las víctimas a sitios web maliciosos.

> *"El atacante aprovecha estrategias de optimización en motores de búsqueda (SEO) para engañar a las víctimas y hacer que accedan a estas páginas a través de resultados de búsqueda manipulados",* explicó el investigador de seguridad Jan Michael Alcantara en un informe.
>
> *"Aunque la mayoría de los sitios de phishing están diseñados para obtener información de tarjetas bancarias, algunos de estos documentos PDF incluyen CAPTCHAs falsificados que inducen a los usuarios a ejecutar comandos maliciosos de PowerShell, lo que finalmente conduce a la instalación del malware Lumma Stealer".*

Se calcula que esta operación de phishing ha impactado a más de 1,150 empresas y más de 7,000 personas desde mediados de 2024, con ataques que afectan principalmente a usuarios en América del Norte, Asia y el sur de Europa, dentro de sectores como la tecnología, los servicios financieros y la manufactura.

Entre los 260 dominios utilizados para alojar estos archivos PDF maliciosos, la mayoría están relacionados con Webflow, seguidos por sitios vinculados a GoDaddy, Strikingly, Wix y Fastly.

Los ciberdelincuentes también han subido algunos de estos archivos PDF a plataformas legítimas de almacenamiento y bibliotecas digitales, como PDFCOFFEE, PDF4PRO, PDFBean e

Internet Archive, para aumentar su alcance a través de búsquedas en línea.

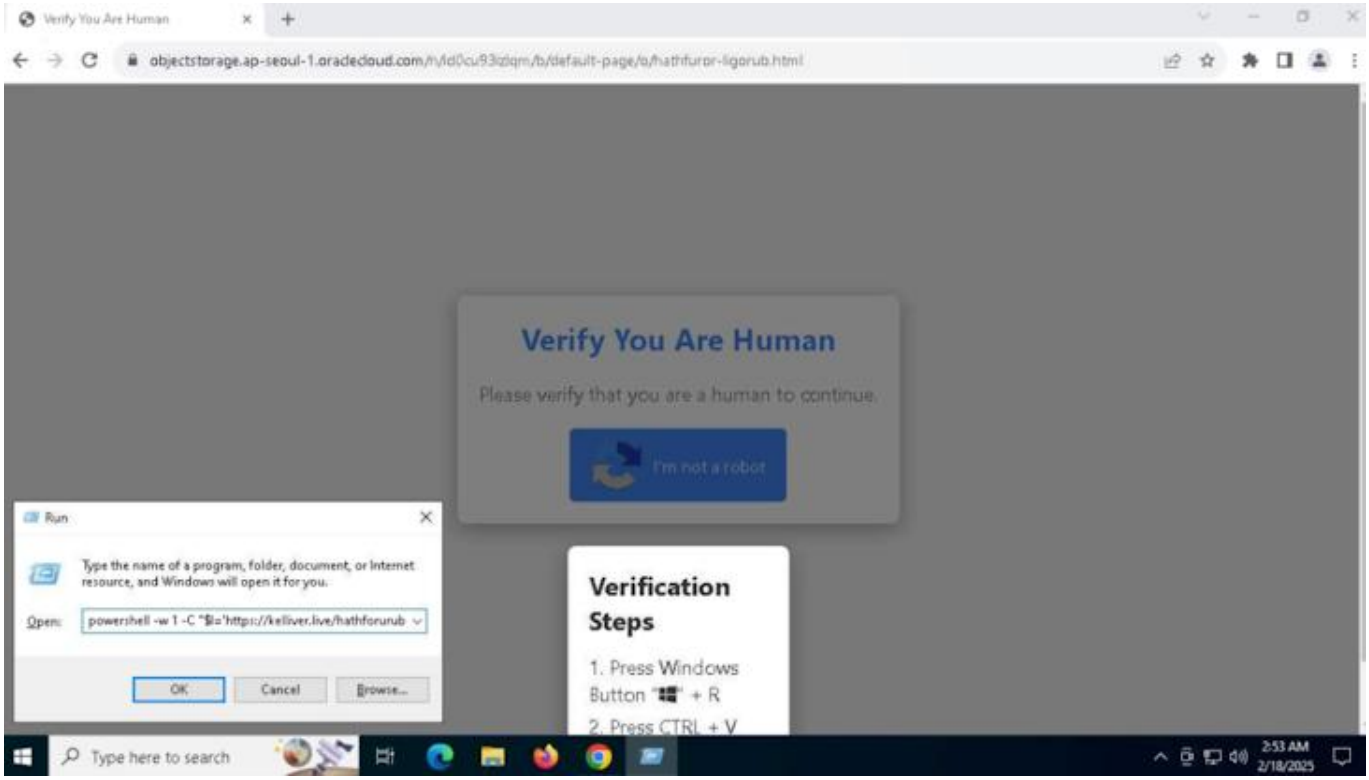
Dentro de estos archivos PDF, se incluyen imágenes fraudulentas de CAPTCHA utilizadas como medio para robar datos bancarios. En otros casos, los documentos diseñados para propagar Lumma Stealer contienen botones de descarga falsos que, al ser presionados, redirigen a la víctima a un portal malicioso.

Los sitios de destino se disfrazan como páginas de verificación CAPTCHA, empleando la técnica *ClickFix* para inducir a los usuarios a ejecutar un comando MSHTA que lanza un script de PowerShell con la intención de instalar el malware.

En semanas recientes, Lumma Stealer también ha sido distribuido mediante archivos disfrazados de videojuegos de Roblox y versiones pirateadas de la herramienta Total Commander para Windows, lo que evidencia la diversidad de tácticas empleadas por actores maliciosos. En muchos casos, los usuarios son conducidos a estos sitios a través de videos en YouTube, probablemente subidos desde cuentas previamente comprometidas.

> *«Los enlaces maliciosos y los archivos infectados suelen camuflarse en videos de YouTube, en los comentarios o en las descripciones. Ser precavido y desconfiar de fuentes no verificadas al interactuar con contenido de YouTube, especialmente cuando se solicita hacer clic en enlaces o descargar archivos, puede ayudar a prevenir este tipo de amenazas»*, advirtió Silent Push.

Además, investigadores en ciberseguridad han detectado que registros robados por Lumma Stealer están siendo compartidos sin costo en un foro de hackers relativamente nuevo llamado *Leaky[.]pro*, que comenzó a operar a finales de diciembre de 2024.



Lumma Stealer es un malware con amplias capacidades que se comercializa bajo el modelo de *malware como servicio* (MaaS), permitiendo la recolección de diversa información de dispositivos con sistema operativo Windows comprometidos. A principios de 2024, los desarrolladores de este malware anunciaron su integración con GhostSocks, un malware proxy programado en Golang.

> *"La incorporación de una función de conexión SOCKS5 en las infecciones de Lumma, o en cualquier otro malware, representa una ventaja significativa para los atacantes"*, señaló Infrawatch.
>
> *«Utilizando las conexiones de internet de las víctimas, los ciberdelincuentes pueden eludir bloqueos geográficos y controles de autenticación basados en direcciones IP, como los implementados por entidades financieras y otros objetivos de alto valor.*

> *Esta capacidad incrementa notablemente la efectividad de los accesos no autorizados mediante credenciales extraídas con infostealers, lo que amplifica el potencial de explotación tras una infección con Lumma».*

Estos hallazgos se dan en un contexto donde otras amenazas como Vidar y Atomic macOS Stealer (AMOS) también han sido propagadas mediante la técnica *ClickFix*, utilizando señuelos relacionados con el chatbot de inteligencia artificial DeepSeek, según informes de Zscaler ThreatLabz y eSentire.

Asimismo, se ha identificado el uso de una técnica de ofuscación en JavaScript que incorpora caracteres Unicode invisibles para representar valores binarios, un método que fue documentado por primera vez en octubre de 2024.

Este mecanismo implica el empleo de caracteres de relleno Unicode, en particular Hangul de medio ancho (U+FFA0) y Hangul de ancho completo (U+3164), para representar los valores binarios 0 y 1, respectivamente, convirtiendo cada carácter ASCII del código JavaScript en su equivalente en Hangul.

> *"Los ataques eran altamente personalizados, incluyendo información no pública, y el código JavaScript inicial intentaba activar un punto de interrupción en un depurador si detectaba que estaba siendo analizado. Además, si identificaba retrasos en la ejecución, interrumpía el ataque redirigiendo a la víctima hacia un sitio web legítimo",* reveló Juniper Threat Labs.