Los ciberdelincuentes han sido detectados escondiendo código malicioso en imágenes para distribuir software malicioso como VIP Keylogger y 0bj3ctivity Stealer en campañas separadas.

> *«En ambas operaciones, los atacantes ocultaron código malicioso dentro de imágenes que subieron a archive[.]org, un sitio de alojamiento de archivos, y emplearon un cargador .NET idéntico para ejecutar las cargas finales,»* explicó HP Wolf Security en su informe Threat Insights Report para el tercer trimestre de 2024.

El ataque comienza con un correo electrónico de phishing que simula ser facturas o pedidos de compra, con el propósito de engañar a los destinatarios para que abran archivos adjuntos maliciosos, como hojas de cálculo de Microsoft Excel. Cuando estos archivos son abiertos, aprovechan una vulnerabilidad conocida en Equation Editor (CVE-2017-11882) para descargar un archivo VBScript.

Este script tiene como objetivo decodificar y ejecutar un comando de PowerShell que descarga una imagen alojada en archive[.]org. Dentro de la imagen, se encuentra un código cifrado en Base64 que se traduce en un ejecutable .NET y se ejecuta.

El ejecutable .NET funciona como un cargador, descargando VIP Keylogger desde una URL específica y activándolo. Esto permite a los atacantes recopilar información confidencial de los sistemas infectados, como pulsaciones de teclas, contenido del portapapeles, capturas de pantalla y credenciales. VIP Keylogger tiene funciones similares a las de Snake Keylogger y 404 Keylogger.

Una campaña diferente ha sido descubierta enviando archivos comprimidos maliciosos por correo electrónico. Estos correos, que se presentan como solicitudes de cotización, buscan engañar a las víctimas para que abran un archivo JavaScript dentro del archivo comprimido, lo que activa un script de PowerShell.

Al igual que en el caso anterior, este script de PowerShell descarga una imagen desde un

servidor remoto, descifra el código Base64 que contiene y ejecuta el mismo cargador basado en .NET. Sin embargo, en este caso, la cadena de ataque termina con la instalación de un ladrón de información llamado 0bj3ctivity.

Las similitudes entre ambas campañas indican que los ciberdelincuentes están utilizando kits de malware que les permiten aumentar la efectividad de los ataques, mientras reducen el tiempo y las habilidades técnicas necesarias para llevarlos a cabo.

HP Wolf Security también señaló que se ha identificado el uso de técnicas de «contrabando de HTML» (HTML smuggling) para propagar el troyano de acceso remoto (RAT) XWorm a través de un instalador AutoIt, continuando una táctica ya utilizada en campañas anteriores con AsyncRAT.

> *«Es interesante notar que los archivos HTML mostraban indicios de haber sido creados con la ayuda de herramientas de GenAI. Esto demuestra un aumento en el uso de GenAI para las etapas iniciales de acceso y distribución de malware en las cadenas de ataque»,* comentó HP.
>
> *«Los actores maliciosos están aprovechando GenAI para obtener diversas ventajas, como escalar los ataques, generar variaciones que aumenten las tasas de infección y dificultar la identificación de los responsables por parte de los equipos de seguridad».*

Además, se ha observado a los ciberdelincuentes crear repositorios en GitHub que promueven herramientas para hacer trampas en videojuegos con el objetivo de distribuir el malware Lumma Stealer mediante un cargador basado en .NET.

> *«Las campañas analizadas son una prueba más de la creciente comercialización del cibercrimen. A medida que los kits de malware se vuelven más accesibles,*

> *económicos y fáciles de usar, incluso personas con conocimientos limitados pueden construir cadenas de infección altamente efectivas»,* explicó Alex Holland, investigador principal en el laboratorio de seguridad de HP.