Investigadores en ciberseguridad han descubierto una campaña de malware innovadora que utiliza Google Sheets como un mecanismo de comando y control (C2).

La actividad, identificada por Proofpoint a partir del 5 de agosto de 2024, se presenta como si fuera de autoridades fiscales de gobiernos en Europa, Asia y EE. UU., con la intención de atacar a más de 70 organizaciones globales mediante una herramienta personalizada llamada Voldemort, diseñada para recopilar información y entregar cargas maliciosas adicionales.

Los sectores afectados incluyen seguros, aeroespacial, transporte, educación, finanzas, tecnología, industria, salud, automotriz, hospitalidad, energía, gobierno, medios de comunicación, manufactura, telecomunicaciones y organizaciones de beneficios sociales.

Esta campaña de presunto ciberespionaje no ha sido atribuida a un grupo de amenazas específico. Se estima que se han enviado hasta 20,000 correos electrónicos como parte de estos ataques.

Estos correos electrónicos se hacen pasar por autoridades fiscales de EE. UU., Reino Unido, Francia, Alemania, Italia, India y Japón, advirtiendo a los destinatarios sobre cambios en sus declaraciones de impuestos y alentándolos a hacer clic en URLs de Google AMP Cache que redirigen a una página intermedia.

Esta página verifica la cadena User-Agent para determinar si el sistema operativo es Windows y, de ser así, utiliza el manejador del protocolo search-ms: URI para mostrar un archivo de acceso directo de Windows (LNK) que simula ser un archivo PDF utilizando Adobe Acrobat Reader, con el objetivo de engañar a la víctima para que lo ejecute.

> *«Si se ejecuta el archivo LNK, invocará PowerShell para ejecutar Python.exe desde un tercer recurso WebDAV en el mismo túnel (\library), pasando un script de Python en un cuarto recurso (\resource) en el mismo host como argumento»,* explicaron los investigadores de Proofpoint Tommy Madjar, Pim Trouerbach y Selena Larson.

> *«Esto permite que Python ejecute el script sin necesidad de descargar archivos en la computadora, ya que las dependencias se cargan directamente desde el recurso WebDAV.»*

El script de Python está diseñado para recopilar información del sistema y enviar los datos, codificados en Base64, a un dominio controlado por los atacantes. Luego, muestra un PDF señuelo al usuario y descarga un archivo ZIP protegido con contraseña desde OpenDrive.

Este archivo ZIP contiene dos archivos: un ejecutable legítimo llamado «CiscoCollabHost.exe», vulnerable a la carga lateral de DLL, y una DLL maliciosa denominada «CiscoSparkLauncher.dll» (también conocida como Voldemort) que se carga lateralmente.

Voldemort es una puerta trasera personalizada escrita en C que tiene capacidades para recopilar información y cargar cargas útiles adicionales. El malware utiliza Google Sheets para C2, exfiltración de datos y ejecución de comandos por parte de los operadores.

Proofpoint describió la actividad como alineada con amenazas persistentes avanzadas (APT), pero con indicios de cibercrimen debido al uso de técnicas comunes en el entorno del e-crimen.

> *«Los actores de amenazas explotan los URIs de esquema de archivo para acceder a recursos de intercambio de archivos externos, específicamente WebDAV y Server Message Block (SMB). Esto se logra utilizando el esquema 'file://' y apuntando a un servidor remoto que aloja el contenido malicioso»,* señalaron los investigadores.

Este enfoque se ha vuelto cada vez más común entre las familias de malware que actúan como intermediarios de acceso inicial (IABs), como Latrodectus, DarkGate y XWorm.

Además, Proofpoint pudo leer el contenido de la hoja de Google, identificando un total de seis víctimas, incluyendo una que se cree que es un entorno de pruebas o un *«investigador*

conocido.»

La campaña ha sido calificada como inusual, lo que sugiere que los actores de amenazas lanzaron un ataque amplio antes de centrarse en un grupo más reducido de objetivos. También es posible que los atacantes, con diferentes niveles de experiencia técnica, planearan infectar varias organizaciones.

> *«Aunque muchas de las características de la campaña coinciden con la actividad de amenazas cibercriminales, creemos que es probable que se trate de una actividad de espionaje destinada a apoyar objetivos finales aún desconocidos»,* afirmaron los investigadores.
>
> *«La combinación Frankensteiniana de capacidades inteligentes y sofisticadas, junto con técnicas y funcionalidades muy básicas, dificulta evaluar el nivel de habilidad del actor de amenazas y determinar con alta certeza los objetivos finales de la campaña.»*

Este hallazgo coincide con el descubrimiento de una versión actualizada del malware Latrodectus (versión 1.4) por Netskope Threat Labs. Esta versión incluye un nuevo punto final de C2 y dos nuevos comandos de puerta trasera que permiten descargar código shell desde un servidor especificado y recuperar archivos desde una ubicación remota.

> *«Latrodectus ha evolucionado rápidamente, añadiendo nuevas funciones a su carga útil. Comprender las actualizaciones aplicadas a su carga útil permite a los defensores mantener adecuadamente configuradas las tuberías automatizadas y usar esta información para buscar nuevas variantes»*, señaló el investigador de seguridad Leandro Fróes.