La solución de sistema de archivos descentralizado conocida como IPFS, se está convirtiendo en el nuevo *«semillero»* para alojar sitios web de phishing, según informaron investigadores de seguridad cibernética.

La compañía de seguridad cibernética Trustwave SpiderLabs, que reveló detalles de las campañas de spam, dijo que identificó no menos de 3000 correos electrónicos que contenían URL de phishing de IPFS como un vector de ataque en los últimos tres meses.

IPFS, abreviatura de InterPlanetary File System, es una red peer-to-peer (P2P) para almacenar y compartir archivos y datos usando hashes criptográficos, en lugar de URL o nombres de archivo, como se observa en un enfoque tradicional de cliente-servidor. Cada hash forma la base de un identificador de contenido único (CID).

La idea es crear un sistema de archivos distribuido resistente que permita que los datos se almacenen en varias computadoras. Esto permitiría acceder a la información sin tener que depender de terceros, como los proveedores de almacenamiento en la nube, lo que la haría resistente a la censura.

> *«Eliminar el contenido de phishing almacenado en IPFS puede ser difícil porque incluso si se elimina en un nodo, aún puede estar disponible en otros nodos»,* dijeron los investigadores de Trustwave, Karla Agregado y Katrina Udquin.

Lo que complica más las cosas es la falta de un identificador uniforme de recursos (URI) estático que se pueda usar para ubicar y bloquear una sola pieza de contenido cargado de malware. Esto también significa que podría ser mucho más difícil desmantelar los sitios de phishing alojados en IPFS.

Los ataques observados por Trust generalmente involucran algún tipo de ingeniería social para bajar la guardia de los objetivos con el fin de persuadirlos para que hagan clic en enlaces IPFS fraudulentos y activen las cadenas de infección.

Estos dominios solicitan a las víctimas potenciales que ingresen sus credenciales para ver un documento, rastrear un paquete en DHL o renovar su suscripción de Azure, solo para desviar las direcciones de correo electrónico y las contraseñas a un servidor remoto.

> *«Con la persistencia de datos, una red robusta y poca regulación, IPFS es quizás una plataforma ideal para que los atacantes alojen y compartan contenido malicioso»*, dijeron los investigadores.

Los hallazgos se producen en medio de un cambio mayor en el panorama de las amenazas por correo electrónico, con los planes de Microsoft para bloquear macros que hacen que los actores de amenazas adapten sus tácticas para distribuir ejecutables que pueden conducir al reconocimiento de seguimiento, robo de datos y ransomware.

Visto de otro modo, el uso de IPFS marca otra evolución en el phishing, brindando a los atacantes otro campo de juego lucrativo para experimentar.

> *«Las técnicas de phishing han dado un salto al utilizar el concepto de servicios en la nube descentralizados mediante IPFS»,* agregaron los investigadores.

> *«Los spammers pueden camuflar fácilmente sus actividades al alojar su contenido en servicios de alojamiento web legítimos o usar varias técnicas de redirección de URL para ayudar a frustrar los escáneres que utilizan la reputación de URL o el análisis de URL automatizado».*

Además, estos cambios también estuvieron acompañados por el uso de kits de phishing listos para usar, una tendencia llamada phishing-as-a-service (PhaaS), que ofrece un medio rápido y fácil para que los atacantes realicen ataques por correo electrónico y SMS.

Se observó una campaña a gran escala descubierta el mes pasado utilizando una plataforma PhaaS de cuatro meses de antigüedad, denominada Robin Banks, diseñada para robar credenciales e información financiera de clientes de bancos conocidos en Australia, Canadá, el Reino Unido y Estados Unidos, según reveló la compañía de seguridad cibernética IronNet.

> *«Si bien la motivación principal de los estafadores que usan este kit parece ser financiera, el kit también pide a las víctimas sus credenciales de Google y Microsoft despuésde viajar a la página de inicio de phishing, lo que indica que también podría ser utilizado por actores de amenazas más avanzados que buscan ganar acceso inicial a redes corporativas para ransomware u otras actividades posteriores a la intrusión»,* dijeron los investigadores.