El grupo Lazarus, asociado con Corea del Norte, ha sido identificado como responsable de una operación activa que emplea ofertas de empleo fraudulentas en LinkedIn dentro de los sectores de criptomonedas y turismo. El objetivo es propagar malware capaz de comprometer sistemas operativos como Windows, macOS y Linux.

De acuerdo con la firma de ciberseguridad Bitdefender, la estafa comienza con un mensaje enviado a través de una plataforma profesional, en el que se promete trabajo remoto, horarios flexibles y una remuneración atractiva.

> *«Cuando la víctima muestra interés, el supuesto proceso de selección avanza, con el estafador solicitando un currículum o incluso un enlace a un repositorio personal de GitHub»,* indicó la compañía rumana en un informe.
>
> *«Aunque pueden parecer solicitudes inofensivas, estos datos pueden ser utilizados con fines malintencionados, como recopilar información personal o darle credibilidad a la conversación».*

Después de obtener los datos requeridos, el ataque entra en una nueva fase, en la que el atacante, haciéndose pasar por un reclutador, proporciona un enlace a un repositorio en GitHub o Bitbucket que supuestamente contiene una versión preliminar de un proyecto de intercambio descentralizado (DEX). Luego, solicita a la víctima que lo revise y dé su opinión.

El código en cuestión incluye un script ofuscado diseñado para descargar una carga maliciosa de la siguiente fase desde api.npoint[.]io. Se trata de un *stealer* de JavaScript compatible con múltiples plataformas, capaz de recolectar información de extensiones de billeteras de criptomonedas instaladas en el navegador de la víctima.

Además de robar información, este *stealer* también actúa como un cargador de malware, descargando una puerta trasera escrita en Python que permite monitorear el contenido del portapapeles, mantener acceso remoto de manera persistente e instalar software malicioso

adicional.

En esta etapa, es importante mencionar que las técnicas documentadas por Bitdefender tienen similitudes con una operación maliciosa conocida como *Contagious Interview* (también llamada *DeceptiveDevelopment* y *DEV#POPPER*), la cual está diseñada para distribuir un *stealer* de JavaScript llamado *BeaverTail* y un implante en Python denominado *InvisibleFerret*.

El malware distribuido mediante este código en Python es un archivo ejecutable en .NET que puede descargar y ejecutar un servidor proxy TOR para establecer comunicación con un servidor de comando y control (C2), extraer información básica del sistema y desplegar otra carga maliciosa que puede robar datos confidenciales, registrar pulsaciones de teclas y ejecutar un minero de criptomonedas.

nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
ejbalbakoplchlghecdalmeeeajnimhm	MetaMask
fhbohimaelbohpjbbldcngcnapndodjp	BNB Chain Wallet
ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom
aeachknmefphepccionboohckonoeemg	Coin98 Wallet
hifafgmccdpekplomjjkcfgodnhcellj	Crypto.com | Onchain
jblndlipeogpafnldhgmapagcccfchpi	Kaia Wallet
acmacodkjbdgmoleebolmdjonilkdbch	Rabby Wallet
dlcobpjiigpikoobohmabehhmhfoodbb	Argent X - Starknet Wallet
mcohilncbfahbmgdjkbpemcciiolgcge	OKX Wallet
agoakfejjabomempkjlepdflaleeobhb	Core | Crypto Wallet & NFT Extension
omaabbefbmiijedngplfjmnooppbclkk	Tonkeeper — wallet for TON
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
nphplpgoakhhjchkkhmiggakijnkhfnd	TON Wallet
penjlddjkjgpnkllboccdgccekpkcbin	OpenMask - TON wallet
lgmpcpglpngdoalbgeoldeajfclnhafa	SafePal Extension Wallet
fldfpgipfncgndfolcbkdeeknbbbnhcc	MyTonWallet · My TON Wallet
bhhhlbepdkbapadjdnnojkbgioiodbic	Solflare Wallet
gjnckgkfmgmibbkoficdidcljeaaaheg	Atomic Wallet
afbcbjpbpfadlkmhmclhkeeodmamcflc	MathWallet

> *«La cadena de infección utilizada por estos ciberdelincuentes es compleja, ya que incluye software malicioso desarrollado en distintos lenguajes de programación y diversas tecnologías. Entre ellas, se encuentran scripts de Python con múltiples capas que se decodifican y ejecutan de manera recursiva, un stealer de JavaScript que primero extrae datos del navegador antes de ejecutar más amenazas, y módulos en .NET capaces de desactivar herramientas de seguridad, configurar un proxy Tor y ejecutar mineros de criptomonedas»,* explicó Bitdefender.

Existen indicios de que estos ataques han sido llevados a cabo de manera extensa, según informes publicados en LinkedIn y Reddit, con ligeras variaciones en la estrategia utilizada.

En algunos casos, a los candidatos se les pide clonar un repositorio Web3 y ejecutarlo localmente como parte del proceso de selección, mientras que en otros se les solicita corregir errores introducidos deliberadamente en el código.

Uno de los repositorios en Bitbucket vinculados a la campaña hacía referencia a un proyecto denominado «miketoken_v2«, aunque ya no se encuentra disponible en la plataforma.

Este hallazgo se produce un día después de que SentinelOne informara que la campaña *Contagious Interview* también está siendo utilizada para propagar otro malware conocido como *FlexibleFerret*.