Lazarus diffonde app DeFi trojanizzate per rubare criptovalute



Lazarus, gruppo APT noto per le motivazioni finanziarie da cui è mosso, ha colpito il settore delle criptovalute attraverso dei Trojan rivolti a nuove app di finanza decentralizzata (DeFi) per aumentare i profitti. Lazarus si serve di applicazioni legittime utilizzate per gestire i portafogli di criptovalute e, tramite esse, diffonde malware che gli conferiscono il controllo sui sistemi delle vittime.

Il gruppo Lazarus, attivo almeno dal 2009, è fra gli attori APT più prolifici al mondo. Contrariamente alla maggior parte dei gruppi APT sponsorizzati dallo stato, Lazarus ed altri threat actor associati a questo APT hanno fatto del guadagno finanziario uno dei loro obiettivi principali. E mentre il mercato delle criptovalute continua a crescere, insieme al mercato dei non-fungible token (NFT) e della finanza decentralizzata (DeFi), Lazarus mette a punto nuovi modi per prendere di mira gli utenti delle criptovalute.

A dicembre del 2021, i ricercatori di Kaspersky hanno scoperto una nuova campagna di malware che, sfruttando un'applicazione DeFi trojanizzata diffusa dal gruppo Lazarus, colpiva il settore della criptovalute. L'applicazione conteneva un programma legittimo chiamato DeFi Wallet in grado di salvare e gestire i portafogli di criptovalute. Una volta eseguita l'app, insieme al programma di installazione dell'applicazione legittima, veniva rilasciato un file dannoso, lanciando il malware attraverso un percorso di installazione trojanizzato. Questo malware generato sovrascriveva poi l'applicazione legittima con l'applicazione troianizzata.

Il malware impiegato in questo schema di infezione è una backdoor ricca di funzionalità, in grado di controllare i sistemi della vittima da remoto. Nel momento in cui ha preso il controllo del sistema, l'attaccante riesce a cancellare file, raccogliere informazioni, collegarsi ad indirizzi IP specifici e comunicare con il server C2. Basandosi sui precedenti attacchi di Lazarus, i ricercatori stimano che le ragioni dietro queste attività criminali siano di natura finanziaria. Dopo aver esaminato le funzionalità di questa backdoor, i ricercatori di Kaspersky hanno scoperto numerose sovrapposizioni con altri strumenti utilizzati dal gruppo Lazarus, in particolare con i cluster di malware CookieTime e ThreatNeedle. Anche lo schema di infezione multistadio è tipico dell'infrastruttura di Lazarus.

Seongsu Park, senior security researcher del Kaspersky Global Research and Analysis Team (GReAT), ha affermato: "*Abbiamo analizzato l'interesse di Lazarus verso il settore delle criptovalute e abbiamo notato che sono riusciti a sviluppare metodi sofisticati per adescare le loro vittime senza tuttavia richiamare l'attenzione sul processo di infezione. Le aziende di criptovalute e blockchain continuano ad evolversi e ad attrarre livelli più alti di investimento. Di conseguenza, attirano non solo scammer e phisher, ma anche i "big game hunter", compresi i gruppi APT interessati a guadagni economici. Dal momento che il mercato delle criptovalute continua a crescere, crediamo fermamente che l'interesse di Lazarus verso questo settore non diminuirà facilmente. In una recente campagna, Lazarus ha sfruttato un'applicazione DeFi legittima, l'ha imitata e ha rilasciato un malware: è una tattica piuttosto comune usata nel crypto-hunting. Per questo motivo sollecitiamo le aziende affinché prestino attenzione a link sconosciuti e agli allegati delle email: anche se a un primo impatto possono sembrare innocui, potrebbero in realtà essere fraudolenti.*"

È possibile avere maggiori informazioni sulla nuova campagna

di Lazarus a questo link: Securelist.com.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/lazarus-diffonde-app-defi-trojanizzate-per-rubare-criptovalute/