

Criptovalute, la frode del software di mining sui nostri pc

Durante quest'anno i *miner* di criptovaluta si sono affermati come una delle principali tendenze nel panorama economico finanziario internazionale. Un dato che va letto non solo in termini di valute virtuali e possibili bolle, ma anche di sicurezza e di cyber crimine.

Sono sempre di più i criminali informatici che prendono come obiettivo questo settore, mercato in costante crescita, trainato dal successo di criptovalute come il bitcoin, ormai sulla soglia dei 20 mila dollari di valore.

La scorsa estate un'indagine Chainalysis rivelò che **i danni da phishing per gli investitori in criptovalute ammontavano a 225 milioni di dollari**. Più di 30 mila sono state le vittime, perdendo a testa più di 7.500 dollari.

Si trattava di siti web o social account del tutto simili alle piattaforme di offerta di moneta iniziale (ICO), mezzo molto utilizzato per raccogliere fondi per nuove criptovalute. In tal modo si sollecitava gli investitori ad inviare denaro, che poi veniva illecitamente sottratto.

Una delle tecniche di frode utilizzate ultimamente consiste invece nel creare siti web che offrono agli utenti la possibilità di fare il **download gratuito di versioni pirata di software per pc e applicazioni**. Per risultare più credibili, si legge in un recente *Report* di Kaspersky Lab, *"i criminali hanno utilizzato nomi per i domini simili a quelli reali. Dopo aver scaricato il software, l'utente riceve un archivio che contiene anche un programma di mining. Questo programma viene quindi installato automaticamente insieme al software desiderato"*.

Il funzionamento è così descritto dai ricercatori di cybersecurity: ***“dopo essere stati installati, i miner iniziano a operare silenziosamente sul PC della vittima, generando cripto monete per i criminali. In tutti i casi rilevati, è stato utilizzato il software del progetto NiceHash, che ha recentemente subito una grave violazione della sicurezza informatica con conseguente furto di cripto valuta per milioni di dollari. Alcune delle vittime erano collegate a un pool di mining con lo stesso nome”***.

In termini di danni reali non sembra che questi software pirata siano particolarmente virulenti: *“anche se ad alcune persone potrebbe andar bene che uno sconosciuto diventi più ricco a spese proprie, noi consigliamo agli utenti di opporsi a questi tentativi perché anche se non vengono condotti con software nocivi standard rappresentano comunque un’attività fraudolenta”*, ha affermato **Morten Lehn**, General Manager Italy di Kaspersky Lab.

Sostanzialmente, tali software di *mining* riducono le performance di sistema del dispositivo, in alcuni casi lo rendono anche più vulnerabile ad altri malware e aumentano il consumo di energia elettrica, influenzando inevitabilmente sull’esperienza utente nel suo complesso.

<https://www.key4biz.it/criptovalute-la-frode-del-software-mining-sui-nostri-pc/208698/>