V ČR se šíří program kradoucí kryptoměny, vydává se za mail od DHL. Neotvírejte přílohy

- CZ24 News | 24. září 2021

ČESKO: V Česku se e-mailem šíří škodlivý program, který se zaměřuje na krádeže bitcoinu a dalších kryptoměn. K šíření prostřednictvím spamu zneužívá jméno přepravní společnosti DHL a mexického zpracovatele kovů General de Perfiles. Mezi nejvíce zasažené země patří vedle ČR také Turecko, Spojené státy, Argentina, Velká Británie, Itálie, Řecko, Španělsko a Rumunsko. Uvedla to antivirová firma Avast.

Škodlivý program BluStealer se zaměřuje na krádeže kryptoměn, jako jsou Bitcoin, Ethereum, Monero a Litecoin, z populárních peněženek jako jsou ArmoryDB, Bytecoin, Jaxx Liberty, Exodus, Electrum, Atomic, Guarda a Coinomi. BluStealer monitoruje klávesnici počítače, odesílá dokumenty a obsahuje nástroj pro krádež kryptoměn v jednom. Z kryptopeněženek dokáže ukrást data, jako jsou soukromé klíče a přihlašovací údaje, díky čemuž může oběť ztratit přístup k peněžence. BluStealer také detekuje kryptoadresy zkopírované do schránky a nahradí je útočníkovými předdefinovanými, takže kryptoměny jsou převedeny do kapsy kyberzločince namísto legitimního příjemce.

Avast vystopoval a zablokoval přibližně 12.000 škodlivých e-mailů distribuujících BluStealer. Spamová kampaň DHL rozesílá obětem e-maily napodobující vzhled skutečných zpráv od DHL, aby vzbudily falešný pocit bezpečí. E-mail informuje uživatele o tom, že balíček byl z důvodu nedostupnosti příjemce doručen do centrálního skladu. Příjemce je následně vyzván k vyplnění přiloženého formuláře, aby mohl doručení balíku přeložit na jiný termín. Když se ale pokusí přílohu otevřít, spustí se instalace BluStealeru. V případě General de Perfiles obdrží příjemci e-mailem informaci, že mají přeplatek na fakturách a že jim byl ponechán kredit, který jim bude odečten při dalším nákupu. Stejně jako kampaň DHL obsahuje i zpráva General de Perfiles škodlivou přílohu BluStealer.

“Kryptoměny jsou stále populárnější a podle odhadů burzovní platformy Crypto.com vlastní kryptoměny více než 100 milionů lidí na celém světě. Transakce s kryptoměnami je navíc obtížnější sledovat a rušit. To vše dělá z uživatelů kryptoměn atraktivní cíl pro kyberzločince,” uvedl výzkumník malwaru v Avastu Anh Ho.

Avast doporučuje uživatelům, aby si dávali pozor na e-maily, které tvrdí, že obsahují faktury za dopravu nebo dobropisy, a neotevírali přílohy v nevyžádaných nebo nedůvěryhodných zprávách. “Ke kryptoměnám by se lidé měli chovat jako ke každé jiné měně. Maximální obezřetnost při nakládání s nimi v internetovém prostředí je proto namístě. Základem je používání zabezpečených kryptoměnových peněženek od prověřených poskytovatelů a zejména bezpečné ukládání hesel k nim,” doplnil ředitel obchodníka s kryptoměnami Bit.plus Martin Stránský.