DE IBK

Mesterséges intelligenciával támogatott állásajánlatokhoz kapcsolódó átverések

Az utóbbi időszakban egyre gyakoribbak azok az online csalások, amelyek **állásajánlatnak álcázva** próbálnak rávenni felhasználókat arra, hogy **fertőzött fájlokat töltsenek le és nyissanak meg.** Átlagos felhasználók, álláskeresők, pályakezdők és tapasztalt szakemberek egyaránt célponttá válhatnak, különösen akkor, ha munkahelyi vagy személyes számítógépen kezelik az ilyen jellegű megkereséseket.

A most elemzett kampány egyik különlegessége, hogy a támadók **mesterséges intelligencia segítségével generált kódot és tartalmat használnak**, amellyel meggyőzőbb e-maileket és technikailag összetettebb fertőzési láncokat hoznak létre.

A támadás jellemzően **egy e-maillel indul, amely állásajánlatot, projektmunkát vagy „marketing/stratégiai lehetőséget" ígér**, ismert márkák vagy cégek nevére hivatkozik, professzionális hangvételű, nem feltűnően hibás szöveget használ.

A levél csatolmány helyett, egy **letöltési linket tartalmaz**, amely egy fájlmegosztó oldalra (például Dropboxra) mutat. Ez sok felhasználóban nem kelt gyanút, hiszen a fájlmegosztók legitim, mindennapos eszközök.

A letöltött ZIP vagy RAR fájl neve gyakran kifejezetten „hihető":

- új marketing pozíció,
- termékbevezetési terv,
- fizetési és juttatási csomag,
- készségfelmérő dokumentum.

Az archívumban látszólag egy dokumentum található, valójában azonban egy **futtatható program, amely dokumentumnak álcázza magát**. A **fájlnév és az ikon is ezt sugallja**, így sok felhasználó gondolkodás nélkül megnyitja. A program egy valódi, **ismert alkalmazást indít el** (például PDF-olvasót), közben egy rejtett, **rosszindulatú összetevőt is betölt**. Ez a technika különösen alattomos, mert a felhasználó valóban lát egy megnyíló PDF-et, emiatt könnyen azt gondolhatja, hogy „minden rendben", miközben a háttérben már elindult a fertőzés.

A fertőzési lánc során használt szkriptek és segédprogramok feltűnően strukturáltak, részletesen kommenteltek, több nyelven is ismertetik a lépéseket. **Ez arra utal, hogy a támadók AI-t használnak kódgenerálásra és automatizálásra.** Ennek következményeként a támadások gyorsabban készülnek el, kevesebb technikai tudással is összetett kártevők terjeszthetők, a fertőzési folyamat „letisztultabb", kevesebb hibát tartalmaz.

A kártevő végül további programokat tölt le az internetről, és észrevétlenül tartósan megtelepszik a gépen.

Az ilyen kampányok során terjesztett kártevők célja nem feltétlenül az azonnali rombolás. Sokkal inkább:

- belépési adatok (jelszavak, böngészőben mentett adatok) megszerzése,
- e-mail fiókok, közösségi oldalak átvétele,
- online banki vagy vásárlási visszaélések előkészítése,
- a fertőzött eszköz „eladása” más bűnözőknek további támadásokhoz.

Fontos, hogy egy magánszemély számítógépe is értékes célpont, különösen, ha azon munka, tanulás, ügyintézés vagy online vásárlás zajlik.

Miért működik ez ennyire jól?

- Az álláskeresés érzelmileg érzékeny helyzet.
- A támadók nem sürgetnek feltűnően, inkább „lehetőséget kínálnak”.
- A fájlnevek, dokumentumok és folyamatok ismerősnek tűnnek.
- A Dropbox-szerű letöltés csökkenti a gyanút.
- A megnyíló PDF „megnyugtatja” a felhasználót.

Az AI pedig segít abban, hogy mindez professzionálisabbnak és hitelesebbnek hasson, mint a korábbi, kevésbé kifinomult adathalász próbálkozások.

Néhány alapelv, ami jelentősen csökkenti a kockázatot:

- Ismeretlen feladótól érkező állásajánlatnál soha ne nyissunk meg futtatható fájlt, még akkor sem, ha dokumentumnak tűnik.
- Legyünk különösen óvatosak, ha a „dokumentum” .exe formátumú.
- Külső fájlmegosztóra mutató link esetén mindig gondoljuk végig, hogy miért nem egy hivatalos állásportálon keresztül érkezik az anyag?
- Használjunk naprakész vírusvédelmet, de ne bízzunk kizárólag benne.