Bitdefender avertizeaza: Hackerii au dezvoltat o campanie în care promit victimelor joburi care nu exista în realitate

Specialistii în securitate informatica din cadrul Bitdefender avertizeaza asupra unei campanii de înselatorie care exploateaza sezonul angajarilor de la începutul anului, în care hackerii trimit e-mail-uri care imita procesul de recrutare al unor companii cunoscute ca sa colecteze date sensibile si sa faca plati frauduloase.

Potrivit unui comunicat de presa al companiei, victima e informata ca CV-ul sau a fost, deja, evaluat si aprobat pentru angajare.

"Uneori, mesajul face referire la o platforma de recrutare, iar alteori, vine din senin, fara ca persoana vizata sa fi aplicat vreodata. E-mail-urile includ de regula afirmatii conform carora candidatul se potriveste perfect postului si contin solicitari de confirmare a unui interviu, de rezervare a unui loc sau de continuare a procesului de recrutare. Mesajele releva un tipar coerent: atacatorii se dau drept angajatori mari, cu branduri pe care oamenii le recunosc si în care au deja încredere precum Amazon, Carrefour si chiar sistemul public de sanatate britanic NHS. Hackerii scriu mesajele în mai multe limbi, precum engleza, spaniola, italiana, franceza si sunt adesea ajustate în functie de locul în care se afla destinatarul", se mentioneaza în comunicat.

Specialistii în securitate cibernetica mentioneaza faptul ca, indiferent de limba, structura mesajelor transmise de catre hackeri ramâne aproape identica: aprobare imediata a candidaturii; proces de interviu minimal sau inexistent; butoane de tip "Confirma interviul" sau "Continua"; solicitari de mutare a conversatiei pe WhatsApp, Telegram sau Microsoft Teams.

"E-mailuri tip "recrutare directa": texte lungi, cu ton procedural si autoritar, menite sa imite un proces real de angajare corporatista. Candidatul e informat ca profilul sau a fost deja aprobat si primeste instructiuni detaliate: sa descarce o aplicatie de mesagerie, sa contacteze un "manager de HR" desemnat sau sa foloseasca o platforma externa pentru programarea unui interviu. Odata ce discutia se muta din e-mail, infractorii pot extrage date personale, solicita documente de identitate sau introduce taxe mascate drept costuri de training. E-mailuri de tip "confirmare printr-un singur click": vizual curate, cu putine detalii, logo-ul unei companii cunoscute, un text scurt si butoane proeminente precum "Confirma interviul". Unele includ chiar "mesaje vocale" pe care destinatarul nu le poate însa asculta. Mesajul duce de regula la o pagina falsa care colecteaza date de acces, date sensibile sau redirectioneaza catre continut periculos. Ambele formate mizeaza pe încrederea în branduri cunoscute, senzatia de urgenta si teama de a pierde o oportunitate", explica reprezentantii Bitdefender.

Conform acestora, ceea ce pare o oportunitate de angajare se poate transforma rapid într-un incident de securitate ce duce la furt de date personale si date de acces: CV-uri, acte de identitate, date de contact sau pagini false care colecteaza parole de e-mail, plati frauduloase: solicitari de plata pentru "training", "echipament" sau "taxe de procesare", precum si amenintari informatice: link-uri sau atasamente care imita materiale de interviu, dar care instaleaza amenintari informatice pe dispozitivul victimei.

În context, expertii vin cu o serie de recomandari pentru utilizatori: sa nu se acceseze linkuri din e-mailuri nesolicitate, sa se verifice locul de munca vacant direct pe site-ul oficial de cariere al companiei, respectiv sa se verifice linkurile cu atentie înainte de a fi deschisa orice pagina.