Bitdefender: Hackerii vizeaza companii printr-o înselatorie de recrutare pe LinkedIn

Bitdefender a depistat o noua metoda de atac asupra companiilor, prin intermediul ofertelor false de angajare postate pe platforma LinkedIn, dupa ce atacatorii au contactat tocmai un cercetator al companiei, astfel fiind descoperit rapid planul fraudulos.

Potrivit unui comunicat de presa, transmis marti, totul începe cu un mesaj atragator: o oportunitate de a colabora la o platforma de schimb de criptomonede descentralizata.

"Detaliile sunt vagi, însa promisiunea unui job flexibil, remote si bine platit poate atrage victime usor de pacalit. Versiuni similare ale acestei escrocherii au fost observate si în alte domenii, precum turismul sau finantele. Daca victima îsi arata interesul, "procesul de recrutare" continua cu solicitarea unui CV sau a unui link catre un repository GitHub personal. Desi aceste cereri par inofensive, acestea pot fi folosite pentru a colecta informatii personale sau pentru a face interactiunea sa para legitima (...) LinkedIn este o platforma pentru profesionisti si cei aflati în cautarea unui loc de munca, însa a devenit si un mediu prolific pentru infractorii cibernetici care profita de credibilitatea acestei retele de socializare. De la oferte de munca false si scheme complexe de înselatorii, pâna la escrocherii si atacuri derulate de actori statali, reteaua este exploatata pentru a manipula aspiratiile profesionale si încrederea utilizatorilor", se arata în comunicat.

Ulterior, dupa ce obtine informatiile dorite, atacatorul trimite un set de fisiere ce contine asa-numitul "Minimum Viable Product" (MVP) al proiectului, împreuna cu un document cu întrebari care pot fi rezolvate doar prin rularea unui demo.

"La prima vedere, codul pare inofensiv. Însa, o analiza mai atenta dezvaluie un script ascuns si dificil de descifrat, care încarca si ruleaza dinamic cod periculos de pe un server extern (...) Odata activata, amenintarea informatica instalata pe sistem poate sa întreprinda urmatoarele actiuni: fura fisiere importante din extensiile vizate ale browserului, colecteaza datele de autentificare stocate în browser, sustrage informatiile catre un server controlat de atacatori. Dupa compromiterea initiala, amenintarea informatica initiaza o serie de actiuni suplimentare pentru a extinde atacul. Înregistreaza apasarile de taste, monitorizeaza clipboard-ul si colecteaza informatii despre sistem, inclusiv fisiere confidentiale si date de autentificare. De asemenea, mentine o conexiune activa cu serverele atacatorilor, ceea ce le permite accesul neautorizat si sustragerea continua a datelor", explica specialistii.

Conform sursei citate, în etapa finala, amenintarea informatica instaleaza componente suplimentare pentru a ocoli solutiile de securitate si a comunica prin retele anonime.

"Analiza tacticilor si a codului periculos indica o amenintare derulata de un actor statal, cel mai probabil gruparea Lazarus (APT 38) din Coreea de Nord. Acesti atacatori nu sunt motivati doar de furtul de date personale. Ei vizeaza persoane din industrii critice - aviatie, aparare, energie nucleara - pentru a obtine acces la informatii clasificate, secrete comerciale si date de acces ale companiilor. Într-un scenariu mai grav, rularea acestui malware pe un dispozitiv dintr-o retea de companie ar putea compromite infrastructura întregii organizatii. Gruparea Lazarus nu se limiteaza doar la escrocherii de recrutare. Au fost detectate tentative în care atacatorii se dau drept specialisti IT si aplica pentru joburi reale, dupa care infiltreaza infrastructurile companiilor pentru a sustrage date sensibile", noteaza producatorul de solutii antivirus.

Ca urmare a acestor incidente, si nu numai, expertii în securitate cibernetica recomanda vigilenta în fata unor

situatii precum: descrieri vagi ale jobului - lipsa unei postari oficiale pe platforma companiei; repositories suspecte - apartin unor utilizatori cu nume aleatorii si nu contin documentatie sau contributii relevante; comunicare slaba - greseli frecvente de scriere si refuzul de a oferi metode alternative de contact, cum ar fi e-mailul de companie sau numere de telefon.

De asemenea, alte sfaturi vizeaza urmatoarele: nu rulati cod neverificat - folositi masini virtuale, sandbox-uri sau platforme online pentru a testa codul în siguranta; verificati autenticitatea - comparati ofertele de munca cu cele de pe site-urile oficiale ale companiilor si verificati domeniile e-mailurilor; fiti precauti - analizati cu atentie mesajele nesolicitate si cererile de informatii personale.

Bitdefender a fost fondata în anul 2001, ofera solutii superioare de preventie, detectie si raspuns la incidente de securitate cibernetica, are clienti în peste 170 de tari si birouri pe toate continentele.