CERT-RO atrage atentia asupra unei campanii de raspândire de malware ce vizeaza clientii unor banci

Specialistii Centrului National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO) atrag atentia asupra unei campanii de raspândire de malware prin intermediul e-mail-ului, ce vizeaza clientii unor banci.

"Clientii unor banci din România continua sa fie tinta atacatorilor cibernetici. Daca saptamâna trecuta, echipa CERT-RO a emis o alerta online despre atacuri de phishing care vizau accesul nepermis la contul utilizatorilor de internet banking, acum dorim sa va atragem atentia asupra unei campanii de raspândire de malware, prin intermediul casutelor de e-mail", se arata într-o postare pe pagina de Facebook a CERT-RO.

Potrivit expertilor în securitate cibernetica, un utilizator primeste pe mail un mesaj în care este informat despre faptul ca s-a efectuat o plata din contul lui, iar în atasamentul anexat acelui e-mail poate accesa ordinul de plata, precum si informatii suplimentare despre tranzactie.

"Sigur, acest mesaj este unul transmis de catre atacatori, conceput pentru a parea ca a fost expediat legitim de catre banca, prin copierea identitatii vizuale (font, logo, adresa), cu scopul de a nu ridica suspiciuni destinatarului. Aflat în fata acestei informatii, utilizatorul se poate speria ca i-au fost sustrasi bani din cont si este posibil sa actioneze pripit, accesând acel atasament malitios din mail, care va duce automat la instalarea unei variante de malware. Atasamentul denumit '□ ordin de plata' nu este un document, asa cum se sustine în e-mail, ci un fisier executabil (.exe), care va instala pe dispozitive varianta de malware denumita 'Agent Tesla'", explica expertii.

Ei atrag atentia ca acest malware care are abilitatea de a înregistra ceea ce tasteaza utilizatorul pe dispozitiv, dar si ce text copiaza pe clipboard, iar aceste informatii sunt transmise mai departe catre un server de comanda si control (C2), manevrat de atacatori. Practic, atunci când utilizatorul se conecteaza pe conturile personale sau ale companiei pentru care lucreaza, acele credentiale pot ajunge în posesia atacatorilor.

Pentru a evita astfel de situatii, echipa CERT-RO recomanda vigilenta, atunci când se actioneaza în mediul online.

"Este important sa fii circumspect deoarece poti primi mesaje-capcana prin diverse canale - e-mail, SMS, retele sociale, apeluri telefonice - de la persoane care pretind a fi angajati ai bancii sau intermediari din partea bancii, sau a altor institutii renumite etc. Analizeaza, înainte de a face clic!", recomanda reprezentantii CERT-RO.

De asemenea, ei îi sfatuiesc pe utilizatori ca, în cazul în care primesc un e-mail sau un mesaj din partea bancii, sa verifice în primul rând sursa mesajului, din header-ul mail-ului (pe cât posibil), deoarece uneori expeditorul real este ascuns, adresa fiind spoofed, dar alteori atacatorii se folosesc de un alias, adresa reala fiind usor vizibila la accesarea sursei acelui mail.

În cazul în care exista suspiciuni cu privire la mesajul primit, clientii bancilor sunt sfatuiti sa verifice informatia, inclusiv validarea transmiterii acesteia catre ei catre, cu expeditorul.

Alte recomandari sunt: folosirea unei solutii de securitate pe dispozitive (antivirus sau antimalware) pentru a scana eventuale link-uri sau atasamente malitioase, mentinerea sistemului de operare si software-ului de pe dispozitive actualizat, efectuare, regulat, de copii de siguranta a fisierelor importante si stocarea acestei copii pe un mediu extern, deconectat de la dispozitiv.