CERT-RO: Recent, clientii companiei de hosting ROMARG au devenit tinta unui atac de tip phishing

Clientii companiei de hosting ROMARG au devenit recent tinta unui atac de tip phishing, prin care utilizatorii serviciilor oferite primesc mesaje privind posibila suspendare a contului, conform unui anunt publicat pe site-ul Centrului National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO.

"Asa cum reiese din alerta publicata de companie, unii dintre clienti ar fi primit e-mail-uri cu subiectul 'Suspensie serviciu', într-o limba româna imprecisa, cu greseli gramaticale sau de exprimare ('pentru a va informa ca contul dvs a fost suspendat'). Asa cum se poate observa dintr-un mesaj primit de clientii ROMARG, e-mail-ul vine de fapt de la o adresa care nu are legatura cu serviciul de hosting (mail1@valeggini.it)", semnaleaza expertii CERT-RO.

Potrivit acestora, atacatorii apeleaza la un element de presiune, urgenta (suspendarea contului pentru neplata serviciului), indus pentru stimularea unei decizii rapide a utilizatorilor. Clientii care doresc reînnoirea serviciului sunt directionati sa acceseze un link din acest e-mail, care contine un 'formular de reînnoire'.

"În realitate, acest formular este creat special de atacatori si gazduit pe o pagina web de pe un site .eu, fara certificat de securitate (http) si fara nicio legatura cu ROMARG. Prin urmare, cei care introduc date pe aceasta pagina transmit aceste informatii atacatorilor", expica expertii în securitate cibernetica.

Alerta publicata de compania de hosting specifica clar faptul ca: ROMARG trimite email-uri legate de contracte si facturi exclusiv la adresa de email asociata contului de client; niciodata la alte adrese; ROMARG nu solicita pe paginile sale introducerea datelor de card, platile online cu cardul putând fi initiate numai din aria de client ROMARG, pe site-ul procesatorului de plati agreat de ROMARG (PayU); Autentificarea în contul de client se face accesând pagina https://www.romarg.ro/cont-client/; Contul de client este disponibil exclusiv la adresa: https://yeti.romarg.com/.

În cazul în care au introdus date legate de cardul bancar pe aceasta pagina de phishing, clientilor li se recomanda sa notifice urgent banca emitenta, pentru a efectua pasii necesari securizarii contului si, în cazul în care sesizeaza ca li s-au extras sume din cont, sa depuna o plângere la politie, pentru deschiderea unei investigatii.

Pentru a evita eventuale riscuri de securitate, ROMARG a decis resetarea parolelor pentru toti clientii, asa cum reiese din alerta publicata pe site.