G Data press release 2016

Comenzi primite pe email ce se dovedesc a fi atacuri de phishing

Atacatorii vizeaza datele de logare ale angajatilor.

Bucuresti (Romania) 28.03.2016

Cazul programului ransomware Locky nu a fost prima incercare de atac efectuata prin e-mail, 54 de milioane de mesaje spam sunt trimise in fiecare zi, in intreaga lume (sursa: Eleven). Acestea nu implica doar atacuri in masa, ci si unele foarte bine directionate. In cazul de fata avem de-a face cu o inselatorie care are tendinta de a viza companii. Procedura este noua. Destinatarii e-mailului pot constata ca aceasta este o incercare de frauda doar in cazul in care sunt foarte atenti. Solutiile de securitate G Data identifica atasamentul ca Script.Trojan-Stealer.Phish.AG. Expertii de securitate de la G DATA Security Labs au dezbatut noua inselatorie in cea mai recenta intrare de pe blog.

Email-ul care ajunge in inbox-urile victimelor se presupune ca este o comanda cu un atasament numit purchase-order.htm, dar, exista totusi indicii in e-mail care indica faptul ca este vorba de o inselatorie. Societatea nu exista sub numele folosit, adresa expeditorului nu este reala, iar textul contine greseli de ortografie. In cazul in care atacatorii obtin accesul la un cont de e-mail care apartine unei persoane fizice sau unei societati, acesta poate fi folosit pentru a trimite mai mult spam. In cazul in care datele de acces ce apartin unei companii ies in exterior, pot aparea probleme grave, cum ar fi accesul neautorizat la datele interne si la e-mailurile companiei.

Fisierul in sine este deghizat in document de tip Microsoft Excel Online, iar in fundal poate fi vazuta o foaie de calcul Excel. Cu toate acestea, este doar o imagine, nu un tabel ce poate fi editat. Imaginea este incarcata de pe un server localizat in Hong Kong. Destinatarii ar trebui sa introduca datele de conectare in formular pentru a incepe descarcarea. Dupa ce se da clic pe "Download", adresa de e-mail si parola introduse sunt trimise catre acelasi server din Hong Kong, din care au fost descarcate imaginile - chiar daca e vorba de un alt domeniu. Acest lucru sugereaza ca intregul server este controlat de catre atacatori. Dupa ce datele au fost trimise, este afisata o pagina web care contine un mesaj de eroare.

Pentru mai multe informatii, puteti viziona G DATA SecurityBlog:
https://blog.gdatasoftware.com/2016/03/28211-order-turns-out-to-be-phishing-attack-in-excel-look

G DATA ofera sfaturi pentru abordarea in siguranta a acestui tip de mesaje

- Utilizati o solutie de securitate comprehensiva si permanent actualizata!

- Utilizati protectie pentru e-mail si protectie antispam-ul pentru a bloca mesajele suparatoare.
- Verificati credibilitatea e-mailurilor. Intrebati-va: Exista vreun motiv pentru care eu sau firma mea ar trebui sa primim aceasta comanda din strainatate? Sunt eu destinatarul acestui e-mail? Ce prima impresie imi lasa acest e-mail? Limba folosita pentru scrierea e-mailului este una des intalnita sau este neobisnuita?
- Ca regula generala, tratati e-mailurile de la expeditori necunoscuti cu suspiciune! In cazul in care un e-mail arata foarte ciudat, iata ce trebuie sa faceti: ignorati-l, stergeti-l si in nici un caz nu deschideti atasamentele si nu dati clic pe link-urile incluse.
- Deschiderea fisierelor atasate implica riscuri necunoscute. Atasamentele ar trebui sa fie mai intai scanate de o solutie de securitate si, daca exista dubii, sterse fara a fi deschise. Daca nu sunteti siguri, trimiteti fisierul la G DATA Security Labs pentru analiza, fara a-l deschide.
- Link-urile din e-mailuri nu ar trebui sa fie accesate fara o evaluare preliminara. Verificati adresa URL. Multe programe de e-mail arata adresa reala atunci cand plasam cursorul mouse-ului deasupra link-ului vizibil, fara sa facem clic pe el - asa-numita functie mouse-over. Daca nu sunteti sigur, trimiteti URL-ul la G DATA Security Labs pentru analiza inainte de a da clic.
- E-mailurile cu atasament fisier HTML ar trebui sa fie tratate cu mult scepticism. Formatul de fisier este utilizat numai pentru site-uri web. Este foarte neobisnuit sa fie folosit pentru schimbul de informatii intre persoane. Acelasi lucru este valabil pentru fisierele in format .js (JavaScript).
- Nu raspundeti niciodata la e-mailuri spam! Un raspuns le indica atacatorilor ca adresa este valabila - si, acest lucru, poate fi chiar mai valoros pentru ei.
- Nu dezvaluiti datele personale - nici pe e-mail, nici in formulare dubioase sau pe pagini web suspecte!
- Ca angajat al unei companii, este important sa discutati cu administratorul IT sau cu CIO daca ceva vi se pare suspect!

-###-