Atac cibernetic cu aplicaţia ransomware PHOBOS

Atac cibernetic cu aplicaţia ransomware PHOBOS

22 iulie 2021

SRI, în cooperare cu CERT-RO și Spitalul Clinic Nr.1 CF Witting din București, a investigat un atac cibernetic cu aplicația ransomware PHOBOS care a vizat serverele entității din domeniul sănătății.

Ulterior criptării datelor, atacatorii au solicitat plata unei răscumpărări pentru decriptarea acestora, plată ce nu a fost realizată de instituția afectată. Cu toate acestea, activitatea curentă a spitalului nu a fost întreruptă, continuitatea fiind asigurată prin utilizarea registrelor offline.

Mai mult, prezentul atac este similar celui din vara anului 2019, când alte 4 spitale din România au fost afectate de PHOBOS, în contextul lipsei unor soluţii antivirus la nivelul infrastructurii IT&C utilizate de acestea.

Ransomware-ul PHOBOS prezintă un nivel de complexitate medie, utilizând ca metodă de infecție, preponderent, conexiunile de tip Remote Desktop Protocol (RDP).

În vederea prevenirii unor atacuri de tip ransomware, experţii Centrului Naţional CYBERINT şi CERT-RO recomandă implementarea unor politici şi măsuri de securitate precum:

- Utilizarea unei soluţii antivirus actualizate;
- Dezactivarea serviciului RDP de pe toate staţiile şi serverele din reţea;
- Actualizarea sistemelor de operare şi a tuturor aplicaţiilor utilizate;
- Schimbarea frecventă a parolelor tuturor utilizatorilor, respectând recomandările de complexitate;
- Verificarea periodică a tuturor utilizatorilor înregistraţi, pentru a identifica utilizatorii noi, adăugaţi în mod nelegitim;
- Realizarea unor copii de siguranţă a datelor critice pe suporţi de date offline;
- Păstrarea datelor criptate în eventualitatea în care ar putea apărea o aplicaţie de decriptare în mediul online.