

Atac cibernetic cu aplicația ransomware PHOBOS

Archived: 2026-04-05 21:23:16 UTC

← ULTIMELE ȘTIRI



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 soluții 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, experții Centrului Național CYBERINT și CERT-RO recomandă implementarea unor politici și măsuri de securitate precum:

- Utilizarea unei soluții antivirus actualizate;
- Dezactivarea serviciului RDP de pe toate stațiile și serverele din rețea;
- Actualizarea sistemelor de operare și a tuturor aplicațiilor utilizate;
- Schimbarea frecventă a parolilor tuturor utilizatorilor, respectând recomandările de complexitate;

- Verificarea periodică a tuturor utilizatorilor înregistrați, pentru a identifica utilizatorii noi, adăugați în mod nelegitim;
- Realizarea unor copii de siguranță a datelor critice pe suporturi de date offline;
- Păstrarea datelor criptate în eventualitatea în care ar putea apărea o aplicație de decriptare în mediul online.

Source: <https://www.sri.ro/articole/atac-cibernet-cu-aplicatia-ransomware-phobos>