# DNSC recomanda cu fermitate ca nimeni sa nu plateasca rascumpararea catre atacatorii sistemului informatic Hipocrate

**Directoratul National de Securitate Cibernetica recomanda cu fermitate ca nimeni sa nu plateasca rascumpararea catre atacatorii sistemului informatic Hipocrate, deoarece plata rascumpararii nu garanteaza ca datele vor fi recuperate si încurajeaza atacatorii.**

DNSC recomanda implementarea urmatoarelor unor masuri de securitate cibernetica cu caracter specific, precum limitarea utilizarii serviciului RDP pe statiile si serverele din retea si adoptarea de masuri suplimentare de securizare a acestui tip de serviciu, utilizarea unor parole complexe si schimbarea periodica a acestora, realizarea unor copii de siguranta a datelor critice si stocarea acestora fie offline, fie pe un segment diferit al retelei, izolarea si pastrarea datelor criptate în eventualitatea în care ar putea aparea o aplicatie de decriptare în mediul online.

De asemenea, specialistii în securitate cibernetica recomanda si implementarea urmatoarelor masuri de securitate cibernetica cu caracter general, precum sporirea vigilentei, care este principalul atu avut oricând la dispozitie de catre un utilizator obisnuit.

"Trebuie manifestata atentie la verificarea e-mail-urilor primite, în special a celor care contin atasamente sau linkuri suspecte! Scanarea cu o solutie de securitate instalata pe dispozitiv, sau cu una disponibila gratis online, pentru linkurile sau atasamentele suspecte din casuta dvs. de mail. Nu uitati sa aplicati la timp update-urile pentru aceste solutii de securitate! E-mail-urile suspecte trebuie raportate departamentului IT pentru izolare si investigare. Verificati periodic regulile contului de e-mail, ce pot fi setate pentru redirectionarea automata a tuturor mesajelor, ceea ce ar putea duce la o scurgere de date, daca exista o infectie", spun reprezentantii DNSC.

Alte masuri ce trebuie avuta în vedere sunt: actualizarea de urgenta a sistemelor de operare, programelor antivirus, browserelor web, clientilor de e-mail si a programelor de tip Office; instalarea unei solutii de control al aplicatiilor (administratorii de sistem pot lua în considerare instalarea unui astfel de software care ofera lista alba de aplicatii si/sau directoare); crearea unor puncte de restaurare a sistemului si realizarea de back-up pentru fisiere; realizarea periodica de sesiuni de training cu personalul.

În cursul noptii de 11 spre 12 februarie 2024 a avut loc un atac cibernetic de tip ransomware asupra companiei Romanian Soft Company (RSC) www.rsc.ro care dezvolta, administreaza si comercializeaza sistemul informatic Hipocrate (alias HIS). Conform datelor DNSC, atacul a perturbat activitatea a 26 spitale din România care utilizeaza sistemul informatic Hipocrate:
Spitalul de Pediatrie Pitesti, Spitalul Judetean de Urgenta Buzau, Spitalul Judetean de Urgenta Slobozia, Spitalul Judetean de Urgenta Pitesti, Spitalul Judetean de Urgenta Târgoviste, Spitalul Judetean de Urgenta "Dr. Constantin Opris" Baia Mare Spitalul Clinic Judetean de Urgenta "Sf. Apostol Andrei" Constanta, Spitalul Clinic Coltea Bucuresti, Spitalul Militar de Urgenta "Dr. Alexandru Gafencu" Constanta, Spitalul Municipal Sighetu Marmatiei, Spitalul Municipal Medgidia, Spitalul de Ortopedie si Traumatologie Azuga, Spitalul Orasenesc Baicoi, Spitalul Clinic de Urgenta Chirurgie Plastica, Reparatorie si Arsuri Bucuresti Spitalul Clinic C.F. nr. 2 Bucuresti, Spitalul de Boli Cronice Sf. Luca, Spitalul de Pneumoftiziologie Rosiorii de Vede, Institutul Clinic Fundeni, Institutul de Boli Cardiovasculare Timisoara, Institutul de Fonoaudiologie si Chirurgie Functionala ORL "Prof. Dr. D. Hociota" Bucuresti, Institutul Oncologic "Prof. Dr. Al. Trestioreanu" Bucuresti (IOB), Institutul Regional de Oncologie Iasi (IRO Iasi), Sanatoriul de Pneumoftiziologie Brad, Centrul medical MALP SRL Moinesti, Centrul Medical Santa Clinic Mitreni (jud. Calarasi), Spitalul de Boli Cronice Smeeni, judetul Buzau.

Malware-ul utilizat în cadrul atacului este aplicatia ransomware Backmydata care face parte din familia de

malware Phobos, cunoscuta pentru propagarea prin conexiuni de tip Remote Desktop Protocol (RDP).

Backmydata este conceput pentru a cripta fisierele tintei vizate utilizând un algoritm complex. Fisierele criptate sunt redenumite cu extensia .backmydata. Dupa criptare, malware-ul furnizeaza doua note de rascumparare (info.hta si info.txt) cu detalii despre pasii ce trebuie urmati pentru contactarea atacatorilor si stabilirea detaliilor pentru plata rascumpararii.

În Romania, sectorul sanatatii a mai fost vizat în 2019 si 2021 de atacuri cibernetice complexe motivate financiar, care au implicat utilizarea malware-ului Phobos.

Phobos cripteaza datele folosind algoritmul AES 256[3] pentru fisiere cu multiple extensii si transmite o nota de rascumparare. Nu exista pâna acum niciun indiciu referitor la exfiltrarea (extragerea, descarcarea) datelor de catre atacatori în acest caz, precizeaza DNSC.

În variantele populare, Phobos îsi opreste executia si se auto-elimina de pe dispozitivele de stocare daca identifica utilizarea de caractere chirilice la nivelul sistemului de operare, aspect comun dezvoltatorilor de malware vorbitori de limba rusa.

Atacatorii utilizeaza platforma getsession în comunicarea cu victimele. Aplicatia foloseste criptarea end-to-end si arhitectura descentralizata pentru a garanta confidentialitatea si a reduce riscul interceptarii mesajelor.