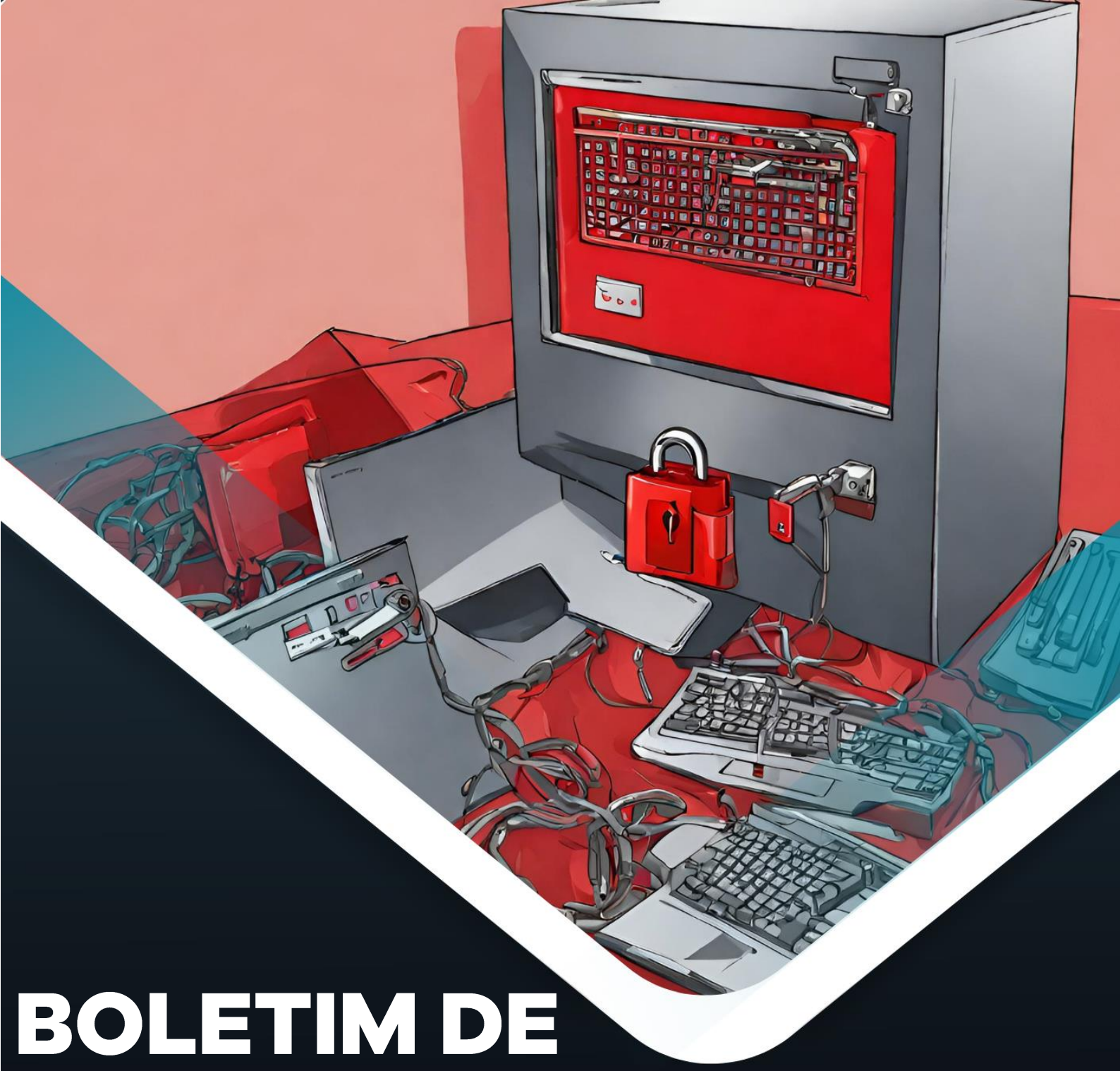


BOLETIM DE SEGURANÇA

100 Hospitais na Romênia afetados por ataque de Ransomware

heimdall
security research
A DIVISION OF ISH

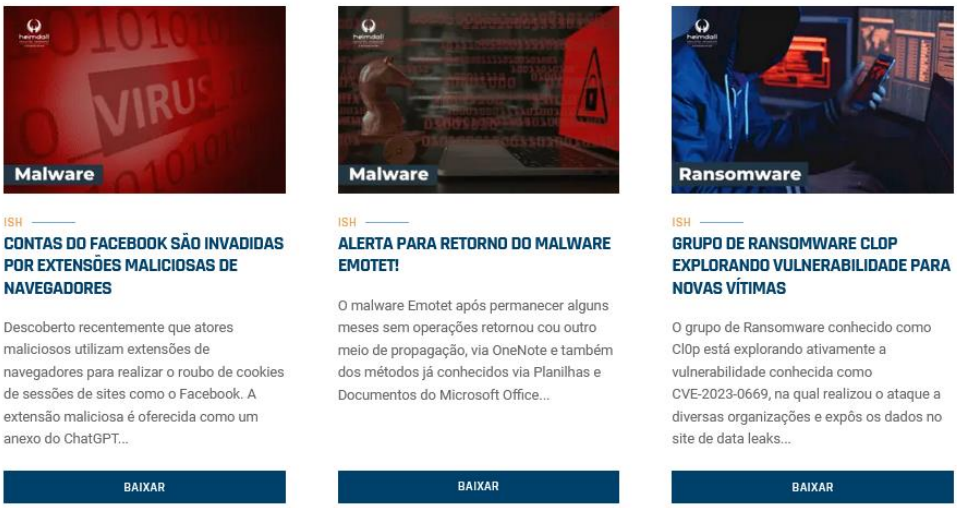
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Mais de 100 hospitais em toda a Romênia ficaram offline devido a um ataque de ransomware que atingiu o sistema de gestão de saúde. O Sistema de Informação Hipócrates (HIS) utilizado por hospitais para gerenciar atividades médicas e dados de pacientes foi alvo do ataque no fim de semana e ficou offline após o banco de dados ser criptografado. De acordo com o divulgado, 25 hospitais teriam sido vítimas dos ransomwares, sendo que as outras 75 unidades vieram a optar por deixar seus sistemas offline por precaução.

De acordo com a nota publicada pelo Ministério da Saúde, durante a noite do dia 11 para 12 de fevereiro de 2024, um ataque de ransomware teve como alvo os servidores de produção que executavam o sistema de informação (HIS).

De acordo ainda com a DNSC (Direção Nacional de Segurança Cibernética), o Ransomware utilizado no ataque é conhecido como “Backmydata”, uma variante da família de ransomware Phobos. É valido salientar que outros grupos de Ransomwares também utilizam a variante do Phobos, como o grupo de ameaças 8base.


MINISTERUL SĂNĂTĂȚII

12 Februarie 2024

Atac cibernetic masiv de tip ransomware asupra serverelor de producție pe care rulează sistemul informatic HIS

În cursul nopții de 11 spre 12 februarie 2024 a avut loc un atac cibernetic masiv de tip ransomware asupra serverelor de producție pe care rulează sistemul informatic HIS. Ca efect al atacului, sistemul este nefuncțional, fișierele și bazele de date sunt criptate.

Unitățile medicale afectate de atacul cibernetic sunt:

Figura 1 – Publicação do Ministério da Saúde da Romênia.

É valido salientar que até o momento não foram obtidos maiores detalhes sobre o ataque realizado pelo ator de Ransomware.

Foram realizadas buscas em fontes abertas e identificado Indicadores de Compromisso (IOC) relacionados ao Ransomware Backmydata, conforme a tabela abaixo:

Indicadores de compromisso do artefato	
md5:	ca52ef8f80a99a01e97dc8cf7d3f5487
sha1:	d4bf7b56d1f022e14a870d724e8da274288bc5db
sha256:	396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6
File name:	AntiRecuvaDB.exe

Tabela 1 – Ransomware Backmydata.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado do Ministério da Saúde da Romênia – Ransomware Backmydata**

heimdall
security research
A DIVISION OF ISH