# ESTUDO DE CASO: ATAQUE DO RANSOMWARE MATRIX/EG83

**Klarissa de Souza Jerônimo[1*], Ivo de Carvalho Peixinho[2]**
[1] Polícia Federal, João Pessoa, Paraíba
[2] Polícia Federal, Brasília, Distrito Federal
**Klarissa de S.Jerônimo; e-mail:* klarissa.ksj@pf.gov.br

**RESUMO**
*O desafio de encontrar autoria de ataques de Ransomware segue em aberto, mas nesses casos as experiências e avanços conseguidos podem auxiliar nessa empreitada dos peritos e demais envolvidos em segurança cibernética.*

**Palavras-chave:** Ransomware, nota de resgate, perícia.

## Introdução

Um ataque do Ransomware Matrix na rede do CREA-PB em 12/08/20 deixou vestígios em servidores secundários que permitiu várias análises periciais: estudo dos logs, demarcação de horários da ação invasora, suspeita da porta de entrada do ataque e, apesar de não ter sido encontrada amostra do programa malicioso, as informações da nota de resgate permitiram achados e análise do ransomware em cooperação com outras fontes de investigação, como relatórios de empresas de antivírus, projetos contra ransomwares.

## Objetivos

Expor perícia de ataque de ransomware em que mesmo não se possuindo a amostra do programa malicioso, encontrou-se alternativa para essa análise e busca de autoria.

## Métodos

Buscou-se amostra do ransomware em "**no more ransom"**, "**id-ransomware"**, entre outros projetos.
A análise de artefato semelhante obtido nessas fontes abertas foi feita com ferramenta automatizada disponível na intranet da PF (malware.pf.gov.br).

## Resultados e Discussão

Apesar de não se ter encontrado o código malicioso no exame pericial, conseguiu-se um artefato semelhante, utilizado em outros ataques, que possuía nota de resgate indicando o mesmo e-mail do caso em questão (evagreps83@yahoo.com). Além disso, a data desse programa semelhante era 30/04/20, bem próxima da data de criação do segundo e-mail divulgado na nota de resgate, 29/04/20, que por sua vez era menos de quatro meses anterior ao ataque.
Sua análise na ferramenta automatizava constatou uma requisição HTTP ao site ghb.timerz.org, enviando nome do computador usuário e outros dados, possivelmente para identificar a chave utilizada na cifragem dos arquivos.
Esse site não estava mais disponível na Internet, porém em consultas do tipo DNS Passivo por IPs que respondiam por ele em datas próximas ao ataque (12/08/20), identificou-se um IP em 27/08/2020 pertencente ao Google na Finlândia. Dada a diferença de mais de um ano entre o ataque e a investigação, não foi continuada a busca pelo proprietário desse IP, apesar de já se ter conseguido respostas de provedores internacionais em casos semelhantes.

## Conclusão

Para casos de Ransomware é importante incentivar a preservação das evidências, a contemporaneidade da investigação ao fato, divulgar as ferramentas disponíveis, as várias fontes de consulta, e no caso dos peritos, análise de laudos anteriores.

## Referências bibliográficas

JERÔNIMO, Klarissa de Souza. Laudo 535/2021-SETEC/SR/PF/PB, de 27/10/2021.
PEIXINHO, Ivo de Carvalho. Resposta do então NUCAT, ao Ofício Nº 482066/2022 - DELEFAZ/DRCOR/SR/PF/PB, de 22/03/2022.