1TDCR Segurança Cibernética – FIAP

NOCRY.

Solução Anti-Ransomware Challenge 2025

São Paulo

9 de Setembro de 2025

*Desenvolvido por: Mateus Mantovani, Maria Clara Cupertino, Lucas Monaco, Pedro Mota, Henrique Buzzuti*

 

Sumário

[1. Introdução 3](#_Toc208334613)

[2. Sprint 1 - proposta inicial (16/03/25) 3](#_Toc208334614)

[3. Sprint 2 - andamento do projeto (20/08/25) 3](#_Toc208334615)

[4. Sprint 3 – primeira entrega final do projeto (9/9/25) 3](#_Toc208334616)

1. Introdução

Este relatório apresenta detalhadamente o encaminhamento e desenvolvimento oficial do projeto de solução Anti-Ransomware desenvolvido pelos alunos mencionados anteriormente neste documento, desde a inicial proposta e plano de construção do software até o atual momento, incluindo alterações, mudanças, incrementações e outros aspectos que foram necessários e decididos em grupo e ordem de melhores e mais rápidos resultados.

1. Sprint 1 - proposta inicial (16/03/25)

Inicialmente o grupo discutiu sobre as bases de um ransomware e de um anti-ransomware, soluções já existentes. Foi elaborada a ideia de desenvolver o anti-vírus em camadas de segurança. Algumas das ideias propostas para a ferramenta foram a inserção de Honeypot, SandBox, Inteligência artificial, sistema de logs, whitelist e EDR para captura do vírus e matar seu processo. Isso tudo foi baseado em pesquisas e estudos iniciantes, pois o grupo estava em fase de compreensão do funcionamento da base do projeto solicitado.

Apesar da proposta, ao decorrer do tempo e desenvolvimento do software, foram analisados e levados em consideração os seguintes pontos:

1. O prazo de entrega era extremamente curto levando em consideração a complexidade do projeto, então o tempo deveria ser investido em fazer o “básico que funciona”
2. Focar em muitos “add-ons” para a ferramenta, deixaria o que já estava complexo ainda mais complexo, levando em consideração que o grupo era composto por alunos iniciantes na área.
3. Para ser eficiente não seriam necessárias tantas ferramentas incrementadas.

E, após discussões e a junção de todos os pontos de vista dos integrantes, concluiu-se que as medidas que deveriam ser tomadas e foram:

1. Cortar HoneyPot

2. Cortar Sandbox

3. Colocar a implementação de IA em segundo plano

4. Dar ênfase em sistema de logs, WhiteList e EDR

5. Desenvolvimento da interface gráfica

1. Sprint 2 - andamento do projeto (20/08/25)

Após a primeira entrega e apresentação do projeto, feedbacks e críticas construtivas da empresa parceira Pride, os próximos passos a serem dados foram........

. Focar mais na literal solução do anti-ransomware

. Dar a maior atenção e prioridade no desenvolvimento do código que realmente iria detectar o ransomware e matar seu processo.

. Interface gráfica, Whitelist, Sistema de logs foram mantidos, pois já estavam prontos.

. A código chave, coração do projeto, foi desenvolvido, mas ainda não está 100% pronto mas já detecta arquivos suspeitos mas segue em construção para melhoras e aprimoramento para matar o processo e evitar cada vez mais os falsos positivos.

1. Sprint 3 – primeira entrega final do projeto (9/9/25)

O plano para esta fase é o aprimoramento da ferramenta e sua eficácia, onde o grupo trabalha cada vez mais para a robustez do projeto, e se o principal for concluído com sucesso, as ferramentas inicialmente propostas serão acrescentadas para sua melhora e evolução.