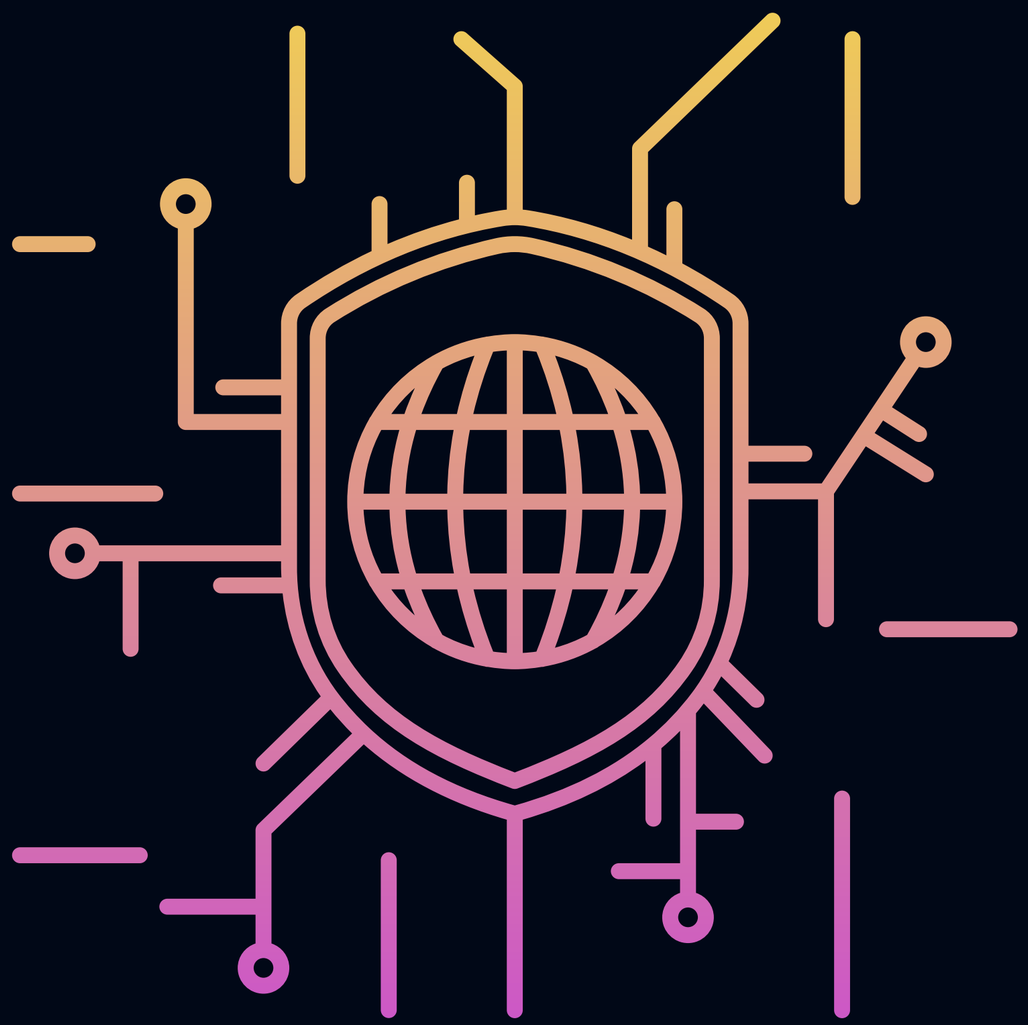


Desenvolvimento de uma Ferramenta de Cibersegurança para Classificação de Malware e Relatório Automático de Ameaças.

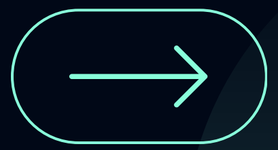
Ransomtracker

ISTEC Instituto Superior de Tecnologias Avançadas do Porto

Índice.

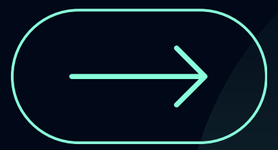
INTRODUÇÃO

O RansomTracker é uma ferramenta avançada preparada para rastrear sites de fraude usados por grupos de ransomware. O projeto tem como objetivo mostrar uma visão abrangente e em tempo real das atividades criminosas na internet, usando AI como ferramenta de complementação do software, permitindo que organizações e indivíduos se mantenham informados sobre ameaças em tempo real e protejam os seus dados de forma eficaz.



Objetivos

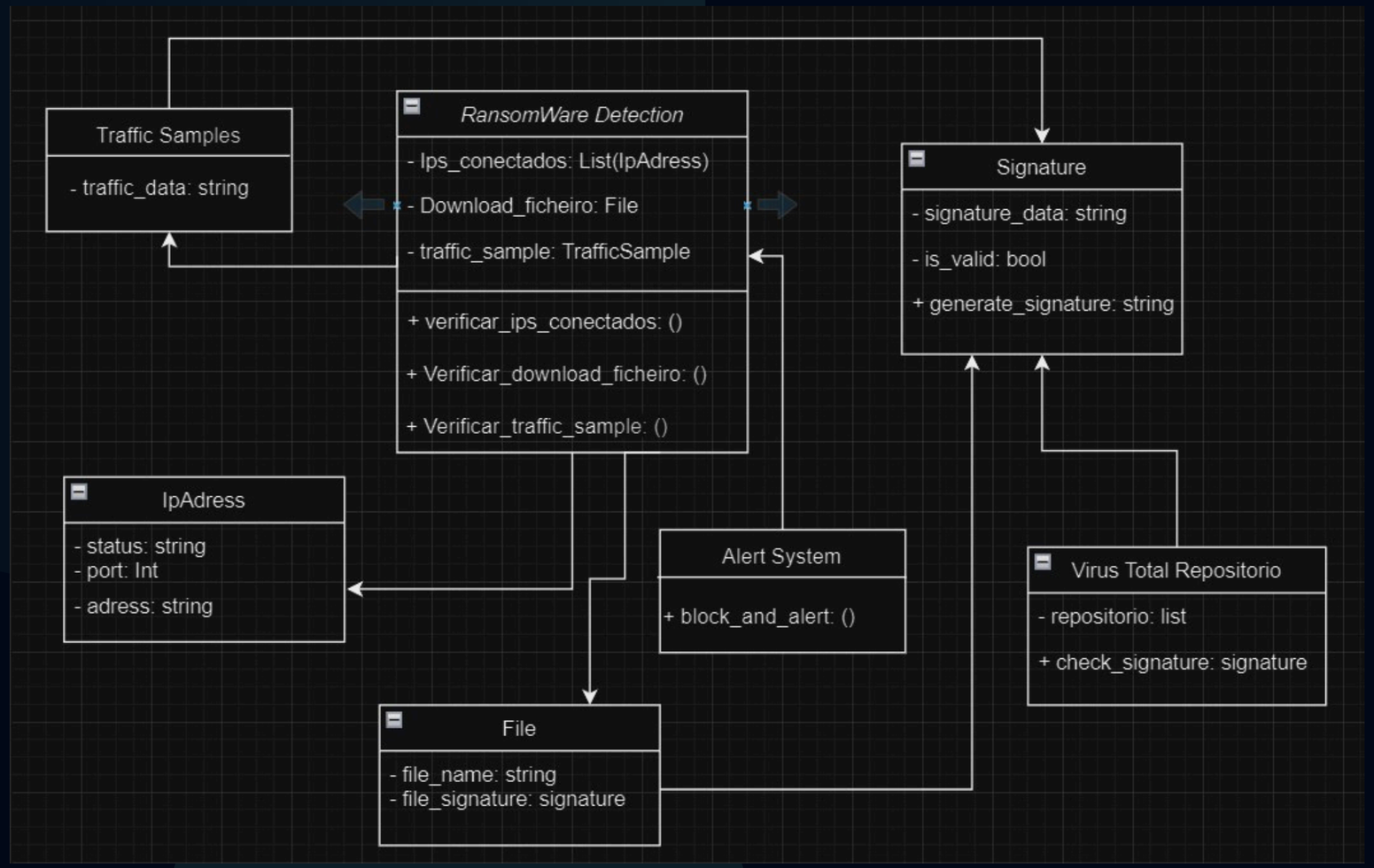
- Monitorar continuamente as atividades de ransomware;
- Fornecer informações atualizadas sobre ameaças em tempo real;
- Ajudar organizações e indivíduos a protegerem seus dados;
- Combate em tempo real de ameaças de malware e ransomware.
- Criar relatórios completos do malware.
- Software de aprendizagem como objetivo conseguir-se adaptar e combater novos malwares.



Ferramentas

- Frontend: React para construção de interfaces interativas;
- Backend : Node.js ou Django para a criação do servidor e API;
- Base de dados:MongoDB ou PostgreSQL para armazenar os dados de rastreamento e de análise;
- Análise de Dados: Python com bibliotecas como Pandas e NumPy para análise de dados;
- Segurança: OWASP ZAP ou Burp Suite para testes de segurança;

UML



Este diagrama UML mostra o sistema de rastreamento de ransomware que:

- **Monitora IPs e tráfego de rede para verificar se estão conectados a endereços suspeitos.**
- **Analisa arquivos baixados e gera assinaturas para compará-los com ameaças conhecidas.**
- **Consulta um repositório de assinaturas para identificar possíveis ameaças.**

Bloqueia e emite alertas quando uma ameaça é confirmada.