

The screenshot shows a dark-themed web application. At the top left is the STEALERX logo. To its right is a blue button labeled "Contribuir com o repositório". Below the logo is a search bar containing the placeholder "exemplo@gmail.com". Underneath the search bar are two green "Informativo" (Informational) cards. The first card, titled "O que é 'Infostealer'?", describes it as a malware that steals information from the victim's computer. The second card, titled "Como se proteger de um Infostealer?", provides guidance on how to protect against it. Below these cards is a section titled "Resultados encontrados" (Results found). It contains a box with the following details:
Data de comprometimento: Dia 12/09/2025 às 12:51:00
Nome do computador: BERSERKER (Jibra)
Sistema Operacional: Windows 11 24H2 build 26100 (64 Bit)
Caminho do Malware: Não encontrado
Antivírus instalados: Não encontrado
IP da máquina: 189.13.*****

STEALERX



powered by
CYBER SHIELD

STEALERX

Cyber Shield

- Matheus Muniz
- Agnaldo da Silva
- Diogo da Silva
- Anderson Godoy
- André Silva
- Loane de Jesus
- Rodrigo Rios
- William Serra
- Tiago Zambelli
- Bruno Silva

Orientador: Rodrigo Amorim Motta Carvalho

Disciplina: Cyber Defense Project: Risk & Vulnerability Analysis



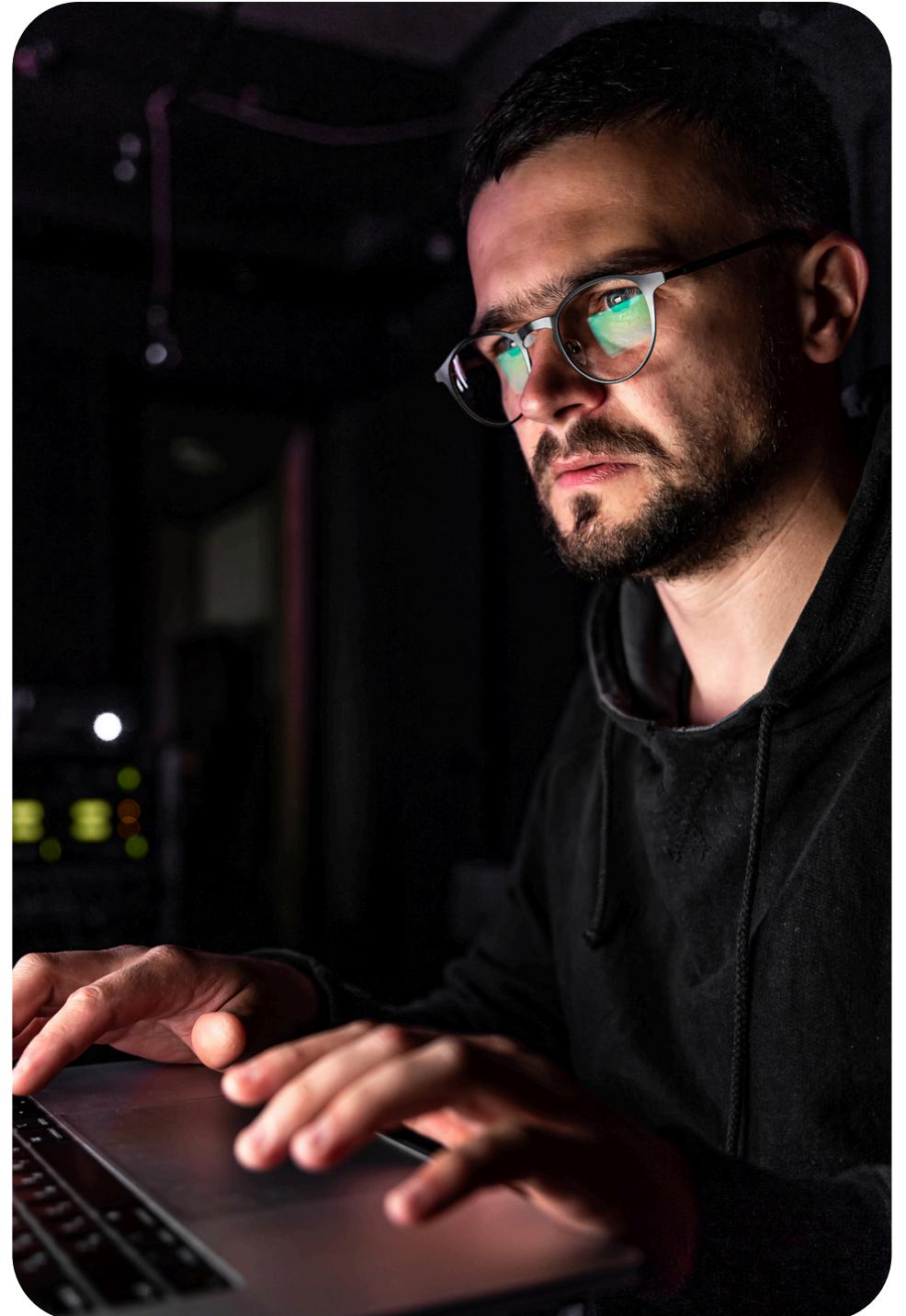
MOTIVAÇÃO

Em 2024, foram registrados 3.158 incidentes de vazamento de dados nos Estados Unidos, de acordo com o relatório anual da Identity Theft Resource Center (ITRC).

Além disso, a SpyCloud destaca que 61% dos vazamentos em 2023 envolveram malware do tipo infostealer, que exfiltra credenciais e dados sensíveis diretamente do dispositivo da vítima.

No Brasil, um relatório da Kaspersky revela que mais de 37 milhões de registros de pessoas físicas e jurídicas foram publicados na dark web em 2024, muitos deles atribuídos a infostealers — incluindo dados pessoais e credenciais de serviços públicos.

Esses números reforçam a urgência e a relevância de uma ferramenta como o StealerX, que permite aos usuários verificarem de forma prática se seus dados foram comprometidos por vazamentos causados por infostealers.

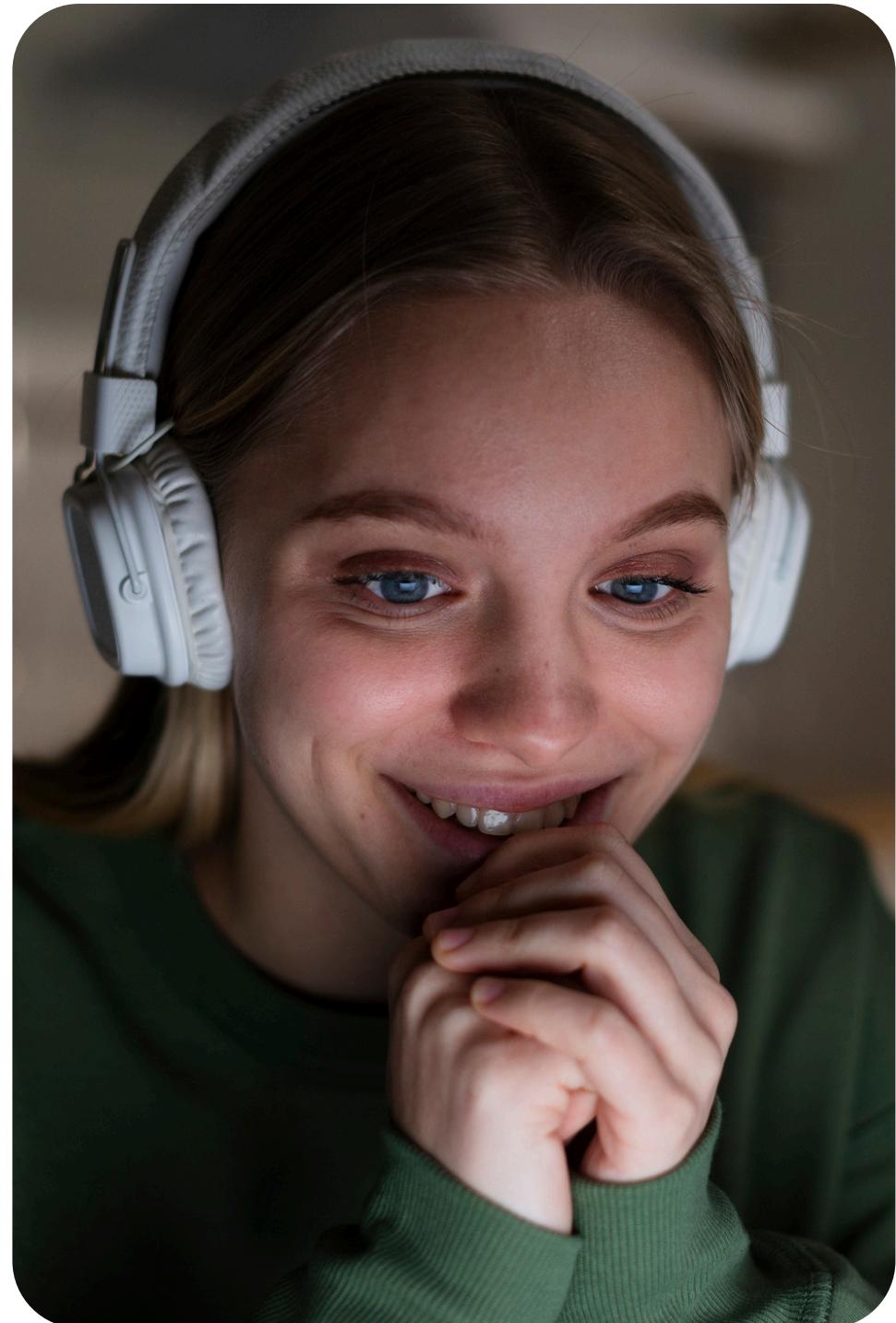


NOSSO OBJETIVO

Os usuários não sabem quando seus dados são roubados por infostealers porque esse tipo de ataque acontece diretamente no dispositivo da vítima. O malware coleta senhas, cookies e outras credenciais em segundo plano, fazendo com que a pessoa continue usando seus serviços normalmente, sem perceber que já teve informações sensíveis comprometidas.

Vazamentos causados por infostealers raramente são comunicados oficialmente, já que eles não dependem de uma invasão a empresas ou sistemas corporativos. Como o roubo ocorre na máquina do usuário, não há organizações responsáveis pela notificação. Isso faz com que milhões de pessoas tenham dados circulando na dark web sem qualquer aviso ou orientação de segurança.

Infostealers crescem como uma das principais origens de credenciais roubadas porque são baratos, fáceis de distribuir e extremamente eficientes. Esse volume de dados alimenta mercados ilegais e facilita golpes como invasão de contas, fraude financeira e sequestro digital.

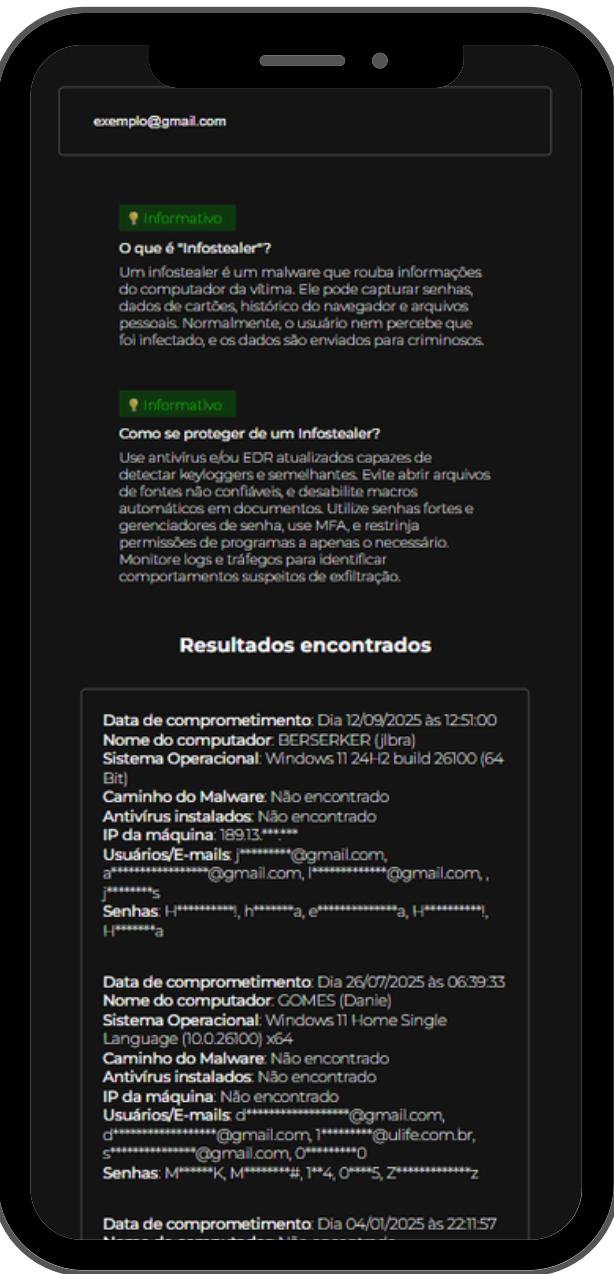


SOLUÇÃO PROPOSTA

A solução proposta pela Cyber Shield foi desenvolver uma aplicação web capaz de identificar, por meio do e-mail do usuário, se seus dados apareceram em vazamentos oriundos de infostealers.

A ferramenta realiza consultas diretas em uma base específica desse tipo de malware, que geralmente não são verificadas por serviços tradicionais de checagem de vazamentos. Dessa forma, o usuário consegue descobrir rapidamente se suas credenciais, cookies ou informações sensíveis foram comprometidas e quais foram, permitindo agir de forma preventiva antes que invasões ou golpes aconteçam.

Sabendo disso, agora mostraremos qual foi a metodologia e a stack (tecnologias) usadas.



powered by
CYBER SHIELD

FLUXO OPERACIONAL

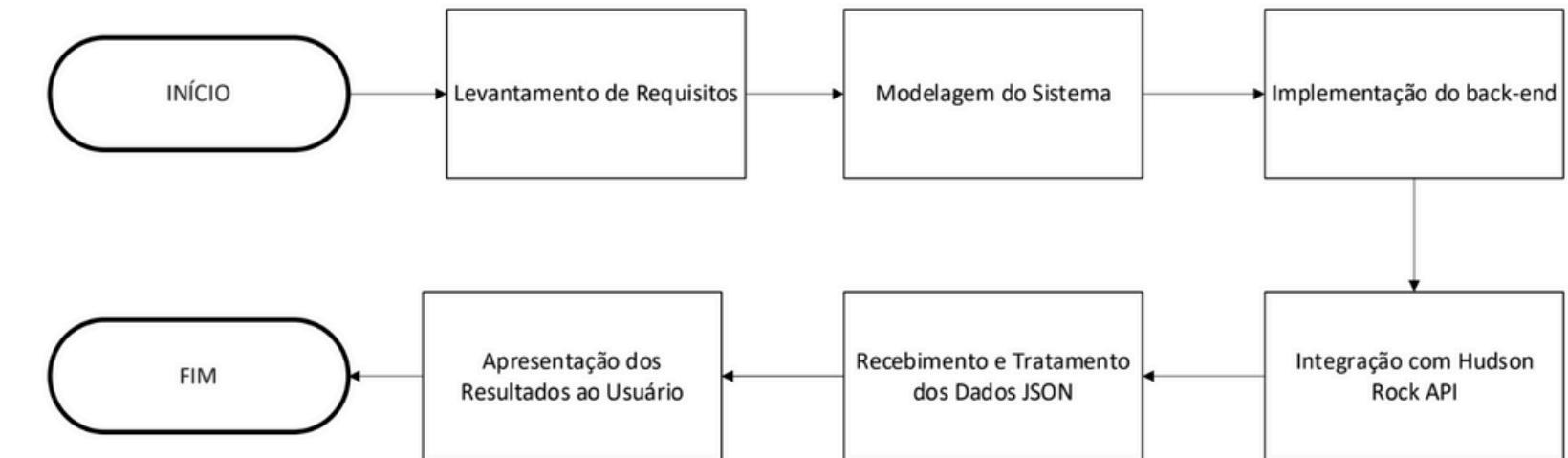
O nosso fluxo operacional do projeto segue uma sequência que vai desde o planejamento até a entrega do resultado ao usuário. Começamos com o levantamento de requisitos, etapa em que são definidas as necessidades do sistema e o que a aplicação deve resolver.

Em seguida, fizemos a modelagem do sistema, estruturando como cada componente irá funcionar e se comunicar, além de como a interface seria.

Em seguida, fizemos a implementação do back-end, responsável por intermediar a comunicação com a API externa — fizemos isso devido a limitações que houve por parte da API—.

Com o back-end consolidado, é feita a integração com a Hudson Rock API, que permite consultar vazamentos provenientes de infostealers.

Após receber as respostas da API, o sistema realiza o tratamento dos dados JSON, organizando e filtrando as informações relevantes. Por fim, esses resultados são apresentados ao usuário de forma clara e acessível, encerrando o fluxo operacional da solução.



O fluxo operacional do StealerX foi estruturado com objetivos que fortalecem a eficiência e o impacto da solução.

Um dos pontos centrais é a capacidade de deduplicar e correlacionar dados, garantindo que informações repetidas sejam eliminadas e que diferentes evidências de comprometimento sejam conectadas para gerar um diagnóstico mais preciso.

A plataforma também prioriza a exibição de resultados claros e açãoáveis, permitindo que o usuário compreenda rapidamente a gravidade do vazamento e saiba exatamente quais medidas tomar.

Além disso, o fluxo foi pensado para reduzir o tempo de resposta a incidentes, acelerando desde a consulta até a interpretação dos dados retornados pela API. Com isso, a organização melhora sua postura de segurança, pois passa a identificar exposições com mais agilidade, reagir de forma preventiva e fortalecer processos internos de proteção contra infostealers e outros vetores de ataque.



TECNOLOGIAS UTILIZADAS

A seleção de tecnologias utilizada no nosso projeto foi definida para garantir desempenho, clareza e facilidade de manutenção.

Python foi escolhido como linguagem principal devido ao seu ecossistema maduro e à ampla disponibilidade de bibliotecas de integração e segurança, permitindo construir um back-end robusto. Para estruturar esse back-end, utilizamos o Flask, que oferece leveza, rapidez na prototipação e documentação consistente, facilitando a criação de endpoints e a integração com serviços externos.

A Hudson Rock - Cavalier API foi incorporada como fonte essencial para a consulta de e-mails em bases de credenciais vazadas, fornecendo ampla cobertura de dados relacionados a infostealers. No front-end, HTML5, CSS3 e JavaScript foram empregados para construir uma interface clara, responsiva e de fácil navegação, garantindo uma boa experiência ao usuário.

GitHub foi utilizado para versionamento e hospedagem do código-fonte, permitindo futuras colaborações, rastreabilidade das mudanças e organização do processo de desenvolvimento.

Tecnologia/Ferramenta	Categoria	Finalidade	Justificativa
Python	Linguagem	Implementação do back-end	Ecossistema maduro, fácil integração com APIs, bibliotecas de segurança.
Flask	Framework Web	Criação de endpoints e integração com APIs	Leve, rápido para prototipação, boa documentação.
Hudson Rock – Cavalier API	API Externa	Fonte OSINT para busca por e-mail	Consulta a bases de credenciais vazadas; cobertura relevante.
HTML5, CSS3, JavaScript	Front-end	Interface do usuário	UI responsiva e clara; rápida iteração.
GitHub	Versionamento e hospedagem	Controle de código-fonte	Colaboração e rastreabilidade.

SEGURANÇA E PRIVACIDADE

O Hudson Rock foi escolhida como fonte principal de consulta porque oferece um padrão de segurança e privacidade superior ao de muitos serviços OSINT disponíveis.

Diferente de plataformas que exibem dados vazados de forma completa (Dehashed, por exemplo), o Hudson Rock censura automaticamente informações sensíveis, como senhas, e-mails completos e até o endereço IP público da máquina comprometida. Esse modelo reduz significativamente o risco de reutilização maliciosa desses dados e impede que a própria busca do usuário gere novas exposições.

Além disso, a API trabalha com identificação baseada em hashes e metadados, permitindo verificar se um e-mail aparece em vazamentos sem revelar o conteúdo integral das credenciais.

Esse conjunto de práticas garante que o StealerX consiga detectar comprometimentos mantendo a privacidade do usuário preservada, alinhado às boas práticas de segurança e ao princípio de exposição mínima.



NA PRÁTICA...

Quando um e-mail é consultado, todas as informações sensíveis retornadas — como nomes de usuário, e-mails e senhas associados ao vazamento — já chegam censuradas pelo próprio Hudson Rock, evitando a exposição integral desses dados. Da mesma forma, o IP público da máquina comprometida também é ocultado, impedindo qualquer uso indevido dessas informações.

Essa censura é essencial porque o projeto não realiza validação ou autenticação de quem está fazendo a consulta, garantindo que nenhum dado sensível seja revelado diretamente ao usuário e mantendo a privacidade e a segurança como prioridades no processo.

Resultados encontrados

Data de comprometimento: Dia 12/09/2025 às 12:51:00
Nome do computador: BERSERKER (jlbra)
Sistema Operacional: Windows 11 24H2 build 26100 (64 Bit)
Caminho do Malware: Não encontrado
Antivírus instalados: Não encontrado
IP da máquina: 189.13.*****
Usuários/E-mails: j*****@gmail.com, a*****@gmail.com, l*****@gmail.com, , j****s
Senhas: H*****!, h*****a, e*****a, H*****!, H*****a



powered by
CYBER SHIELD

REFERÊNCIAS

<https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/>

<https://spycloud.com/newsroom/annual-identity-exposure-report-2024/>

<https://boletimnacional.com.br/2025/07/22/mais-de-37-milhoes-de-dados-de-brasileiros-vazam-na-dark-web-em-2024-aponta-kaspersky/>