SINGAPORE MANAGEMENT UNIVERSITY × OPEN GOVERNMENT PRODUCTS

SCAMSWORD

A set of prototype services that aim to take an offensive approach towards addressing the increasing prevalence of scam cases in Singapore

OUR SOLUTION

CHAT

Scam Chat to actively crowdsource messages from scammers

URL INSPECTION

Inspect URLs for indicators of phishing such as cybersquatting, domain age, and more

CONTENT INSPECTION

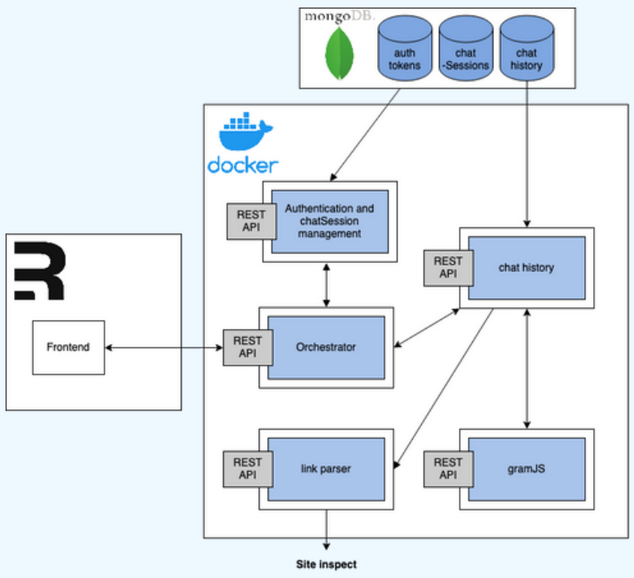
Inspect DOM for XSS and form elements & ML to check for favicon similarity of legitimate sites

TAKEDOWN

Templated Emails sent to providers to takedown malicious websites

ScamSword is an all-in-one application that enables public officers to engage and gather information from scammers through anonymous chats. Any embedded links identified within messages can then be uploaded onto our site inspection service for follow-up. Firstly, we inspect the URL itself, taking note of squatting techniques, domain age and link redirections. We then conduct checks on the site's Document Object Model (DOM) to detect Cross-Site Scripting (XSS) and form input elements. Additionally, our Favicon Similarity Checker compares the site's favicon against a dataset of images collected from legitimate sites. We compile all the information from these checks into a report, and if there is sufficient cause to suspect the link as a phishing site, users can send out templated emails to the relevant Domain Name System (DNS) and/or hosting providers to request takedowns. This proactive approach helps to minimize the risk of members of public falling prey to scams and makes scam operations much more challenging for bad actors.

SYSTEM ARCHITECTURE

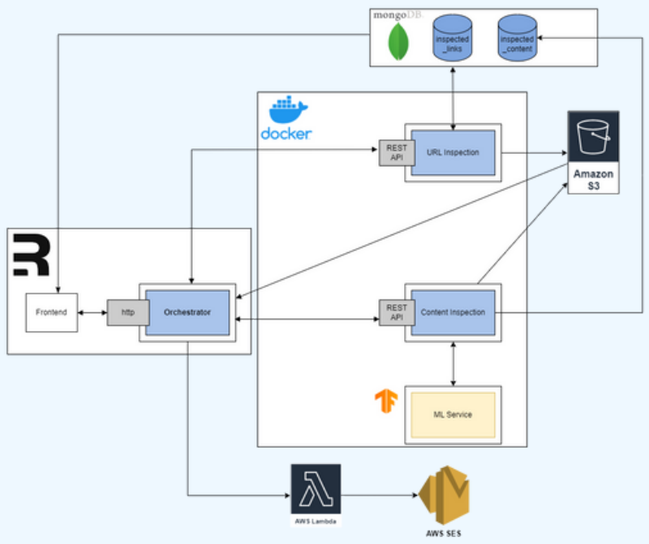


SCAM CHAT

Frontend: Remix
Backend: NodeJS
Database: MongoDB
Infra: AWS ECS

SITE INSPECT

Frontend: Remix
Backend: NodeJS, FastApi
Database: MongoDB
Infra: AWS ECS, Serverless, S3



STAKEHOLDERS

PUBLIC OFFICERS

- Invested in scam prevention and keeping up-to-date with the latest scam operations

OGP

- Seeking to use this project to validate existing hypotheses and inform the implementation of future tools to engage and disrupt scam operations

TAKEAWAYS

CHALLENGES

- Evaluating the performance of different algorithms and determining thresholds
- Integrating the different backend services into a one-stop solution
- Managing differing stakeholder priorities
- Facilitating the flow of messages from the client and Telegram via the backend

LEARNING POINTS

- Effective collaboration, project management tools and teamwork
- Appreciation for the effort required to take a software product from ideation to prototype, and eventually production deployment

X-FACTOR

AI - VGG16 CNN MODEL

- Implemented with TensorFlow, utilizing a pre-trained Convolutional Neural Network (CNN) to judge similarity of favicons

CYBERSECURITY - THREAT INTELLIGENCE

- Integrates knowledge from different bodies of research and publicly maintained datasets to aid the inspection of suspicious sites and lookup of service providers

SAFE PLATFORM TO CHAT WITH SCAMMERS

- The true identities of end users are anonymized through the use of fake accounts, and any potential personal data is automatically filtered from responses

https://github.com/FYP-ScamSword

Charlotte Wee, Claire Liew Xi Wei, Emmanuel Oh, Lee Zhi Xuan, Yun Waddy Soe