## Product Vision

1. Why?

Nowadays there are many fake shops because of increased online interactions due to Covid-19. According to a survey, 40% of respondents (out of 3000 users) admitted that sometimes they are unable to detect on their own whether a certain shop is fake or not, so they need a tool that would protect them. F-Secure already has a product called F-Secure Total that has browsing protection as one of the features, but fake webshop detection is not a part of that product yet, which is where the student team comes in.

There are some solutions for fake webshop detection, such as Google’s Safe Browsing tool, Better Business Bureau’s Scam Tracker tool, but both need a user to visit their website and paste suspicious url in the search field and look through the results. Such procedure assumes that the user is already suspicious and is willing to spend some time to find out whether the site is legitimate. Furthermore, detection algorithm is not public, so it is unclear how accurate those tools are and what features they use. There don’t seem to be a real-time as-you-go solution directly in browser that would appeal to a larger audience who just wants a simple protection tool right when they are looking at some website, and so that user doesn’t have to think about risks and strategies to minimise them. Lack of such solution might be partly explained by the fact that explosion in the number of fake webshops is a recent thing and there is not enough data on them yet. Repurposing existing malicious website detection software to detect fake webshops takes time and effort.

2. What?

Goal: to create a working fake webshop detection pipeline which can be managed in the future. Product is developed for threat analysts. Primary focus is on seamless integration of solid scraping with working interface to access it and with basic extraction and machine learning model. ML model can be adjusted later and its accuracy is a secondary concern. Perfectly accurate machine learning model is beyond Minimum Viable Product.

Minimum Viable Product should include:

* UI to interact with developed solution/platform/pipeline
  + - CLI (command line interface) for internal malware analysts
    - Web UI for analysts who are not comfortable with CLI
    - API that can be used by the web UI and F-Secure Total
* website scraping (bulk scraping, individual scraping, crawling)
* basic extraction of scraped data
* basic machine learning model that can demonstrate that there is working ML model that provides *some* results

End users of F-Secure Total are non-technical people, but since project results are supposed to be integrated into existing F-Secure solution, usability and interface for them is out of scope of this project, as well as detection of any other malicious websites.

Success of product will be measured using the following criteria:

* usability for web interface
* performance and efficiency for bulk scraping and crawling
* accuracy for individual scraping
* speed for extraction
* accuracy for machine learning model
* user feedback for smoothness of pipeline process
* ease of deployment and maintenance in different environments (some malicious fake shops might target only mobile users and do not cause damage if browsed from desktop or vice versa, so website scraping analysis should be able to pick up these differences)
* lack of bugs for testing

(what about Security, adherence to regulations, scalability, reliability, graceful recovery from failure)

3. For Whom?

Users of the product will be malware analysts from F-Secure’s Threat Protection Team (TPT). Some of them are comfortable with command line interface, while others are not, so the end product should have both command line interface and web-based user interface, namely a website / browser extension for Edge, Safari and/or Chrome. Internal users might have different usability requirements compared to non-technical users, and it might be useful to research how developer experience is different from user experience, however user research is not an obligatory step. Some members of the Threat Protection Team will participate in user testing.