WATCHFOX

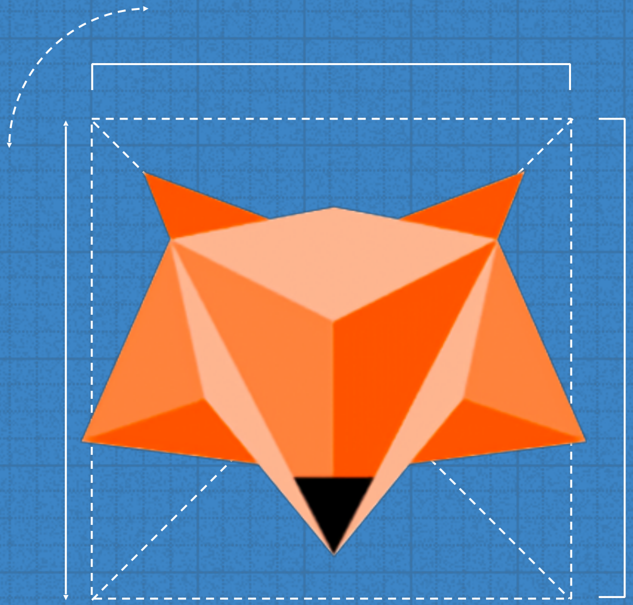
Sophisticated Evaluator

Shuang Wu - Mingjun Yin - Yifan Zhao

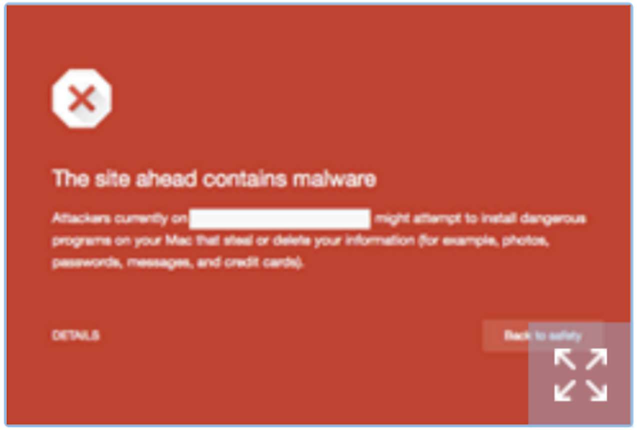
Outline

Watchfox

- Introduction
- Key features
- Project features
- Implementation



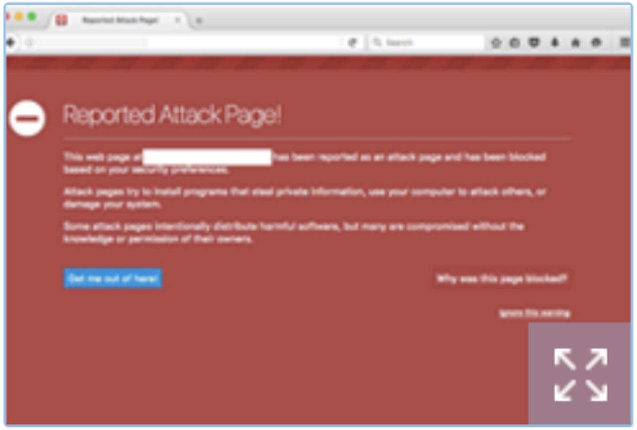
Chrome



The site ahead contains malware

Attackers currently on [redacted] might attempt to install dangerous programs on your Mac that steal or delete your information (for example, photos, passwords, messages, and credit cards).

FireFox



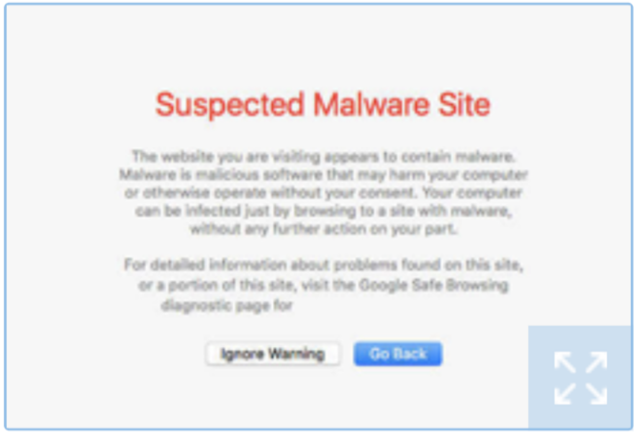
Reported Attack Page!

This web page at [redacted] has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Safari

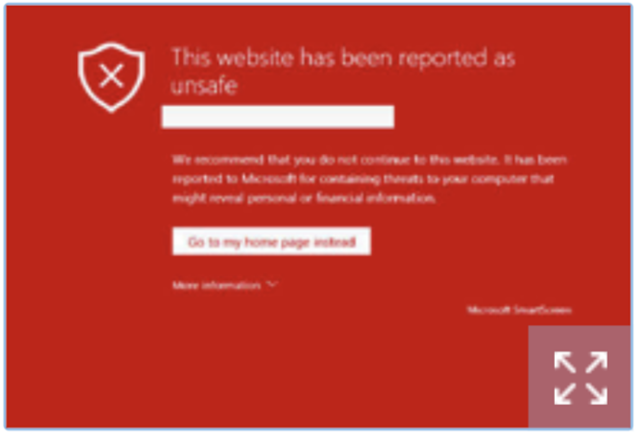


Suspected Malware Site

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for

IE / Edge



This website has been reported as unsafe

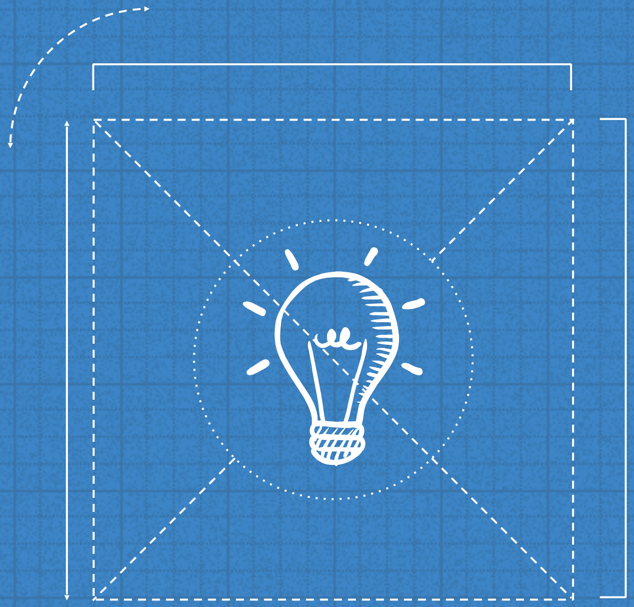
[redacted]

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

Google Blacklist

In order to provide its users a safe online experience, Google has invested resources in identifying and flagging any potentially malicious websites.

To help users know when they're visiting a potentially malicious website they "blacklist" it. This is meant to deter the user from moving forward, notify the website owner, and simultaneously impede the attacker's intentions.



WHY?

Yielding more information

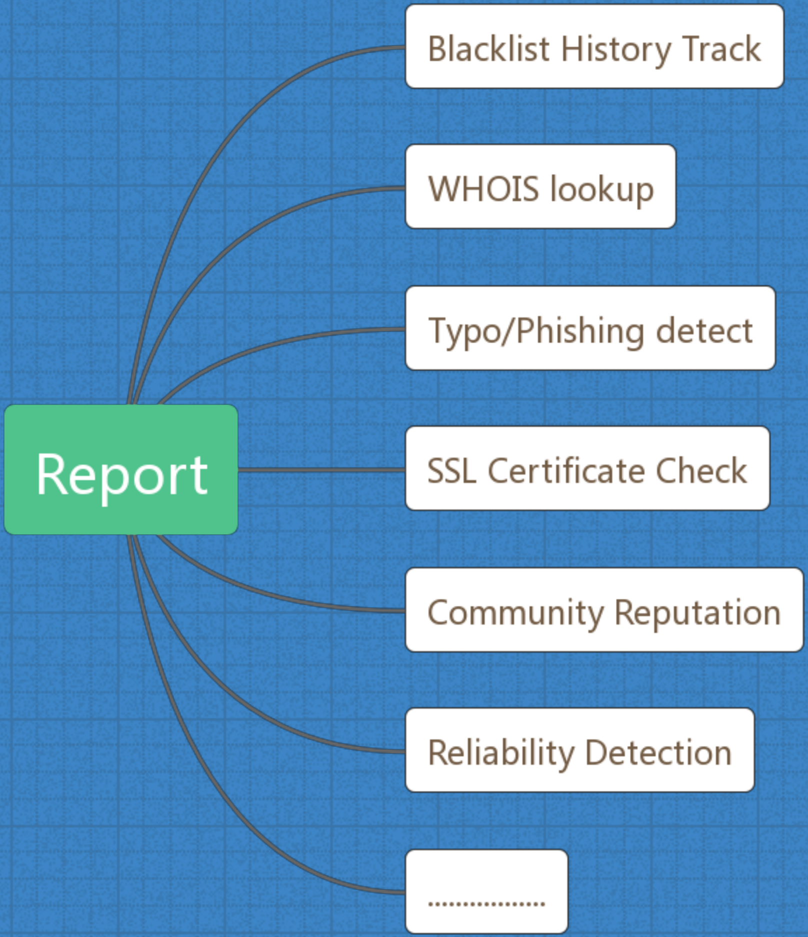
Instead of just one warning

2

INTERFACES

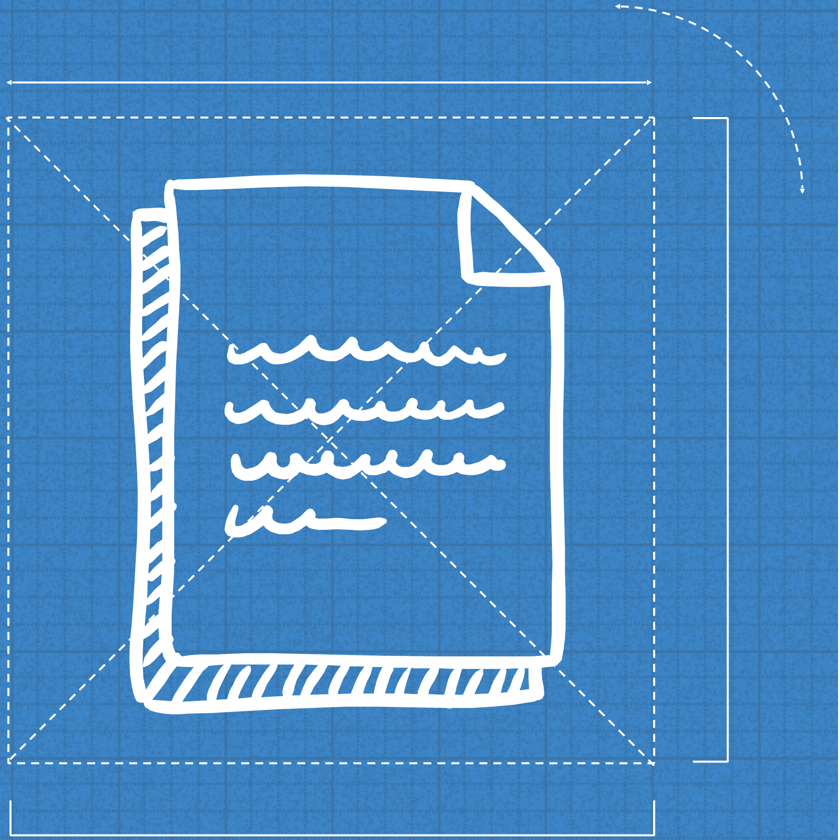
For different purpose of use

FOR NORMAL VIEWERS

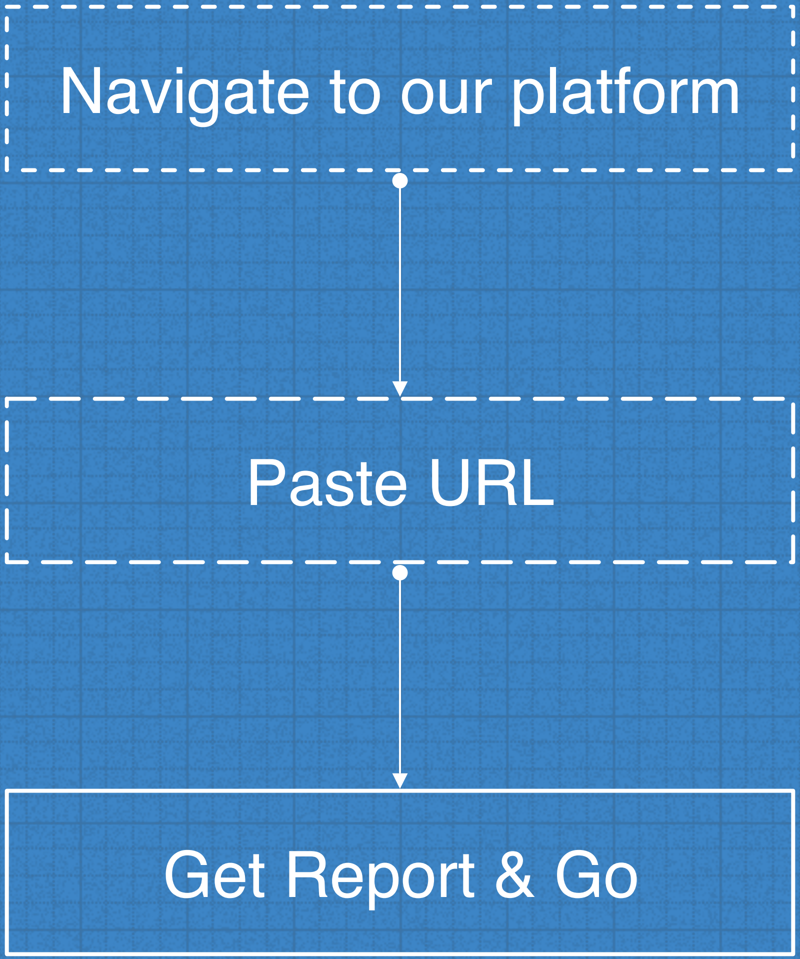


Report

- Blacklist History Track
- WHOIS lookup
- Typo/Phishing detect
- SSL Certificate Check
- Community Reputation
- Reliability Detection
- ....



OUR PROCESS IS EASY

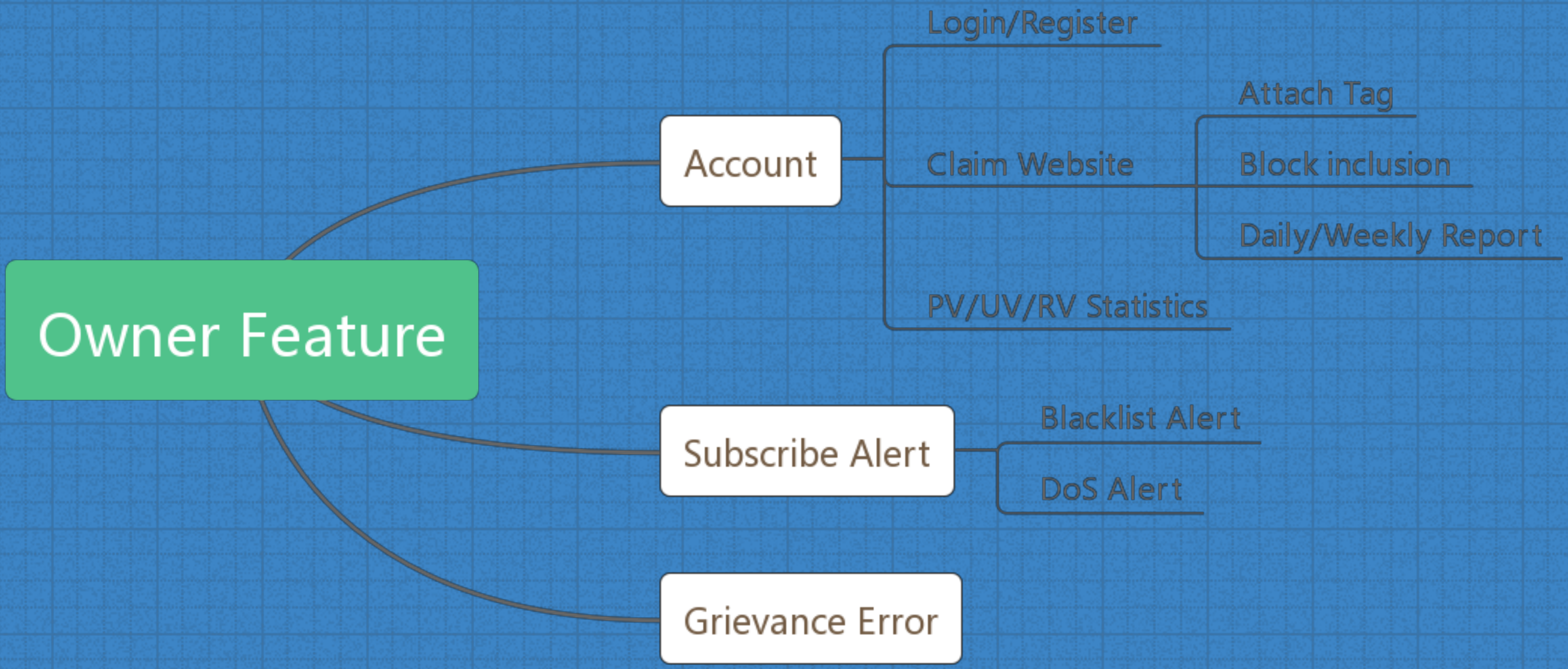


Navigate to our platform

Paste URL

Get Report & Go

For Website Owner



Owner Feature

- Account
  - Login/Register
  - Claim Website
    - Attach Tag
    - Block inclusion
    - Daily/Weekly Report
  - PV/UV/RV Statistics
- Subscribe Alert
  - Blacklist Alert
  - DoS Alert
- Grievance Error

> To competently perform rectifying security service,
> two critical incident response elements are necessary:
> information and organization
>
> —Robert E. Davis

Information - Data Source

Google Blacklist

This is a reliable data source with high accuracy.

WHOIS Database

We can use this to set up our crawler.

MonAPI

This is a large database that contains many details information like geolocation, treat level, ASN number etc.

Crawlers

Apart from existed database, we also maintain our own crawler to meet special requirement of our platform.

5 billion

WHOIS RECORDs

300 million

Active domain names

2,864+

TLDs&ccTLDs

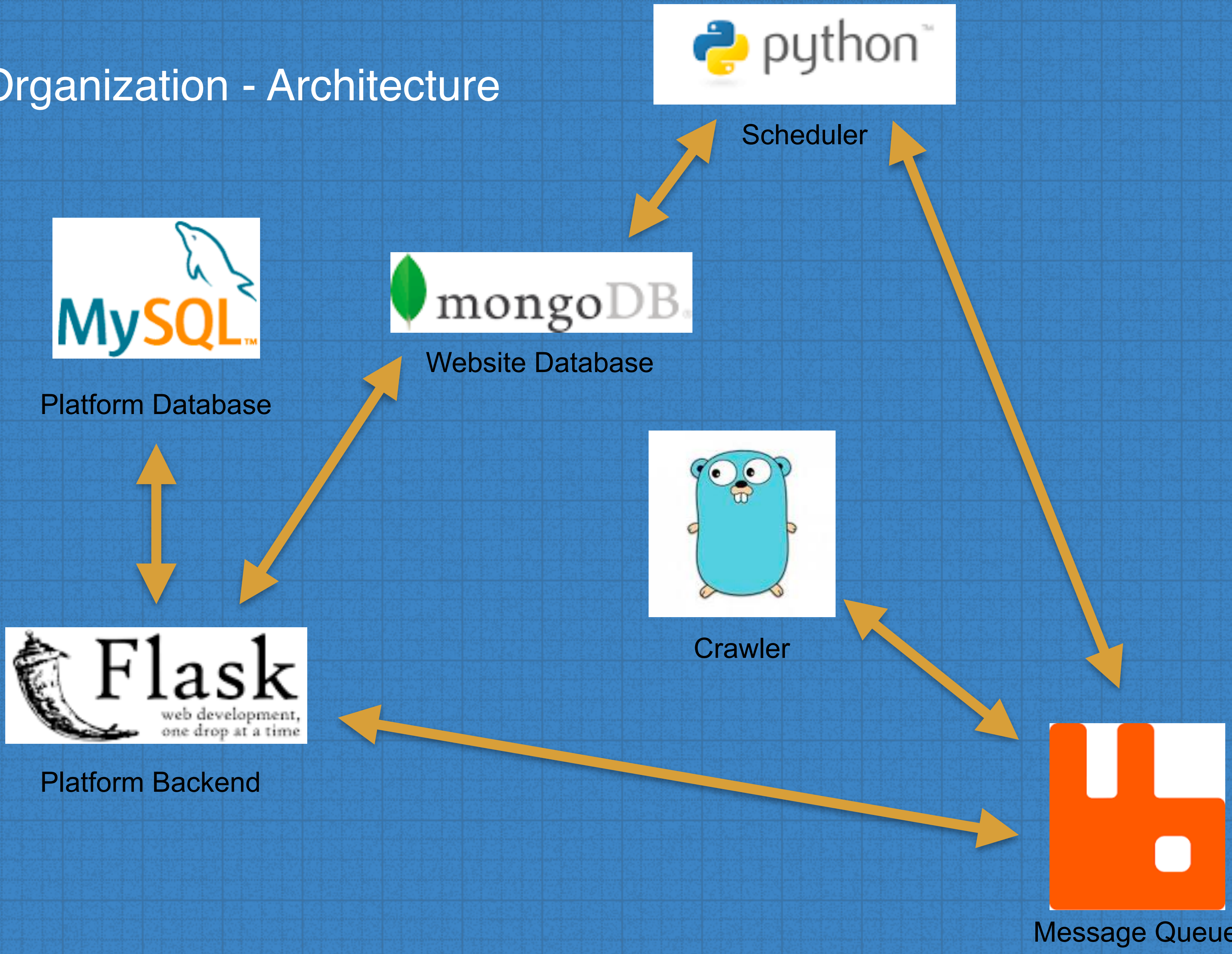
Suppose each domain has 10 URLs on average

3,000,000,000+

URLs

Whoa! That’s a big number,
how can we handle them?

Organization - Architecture



Scheduler

Platform Database

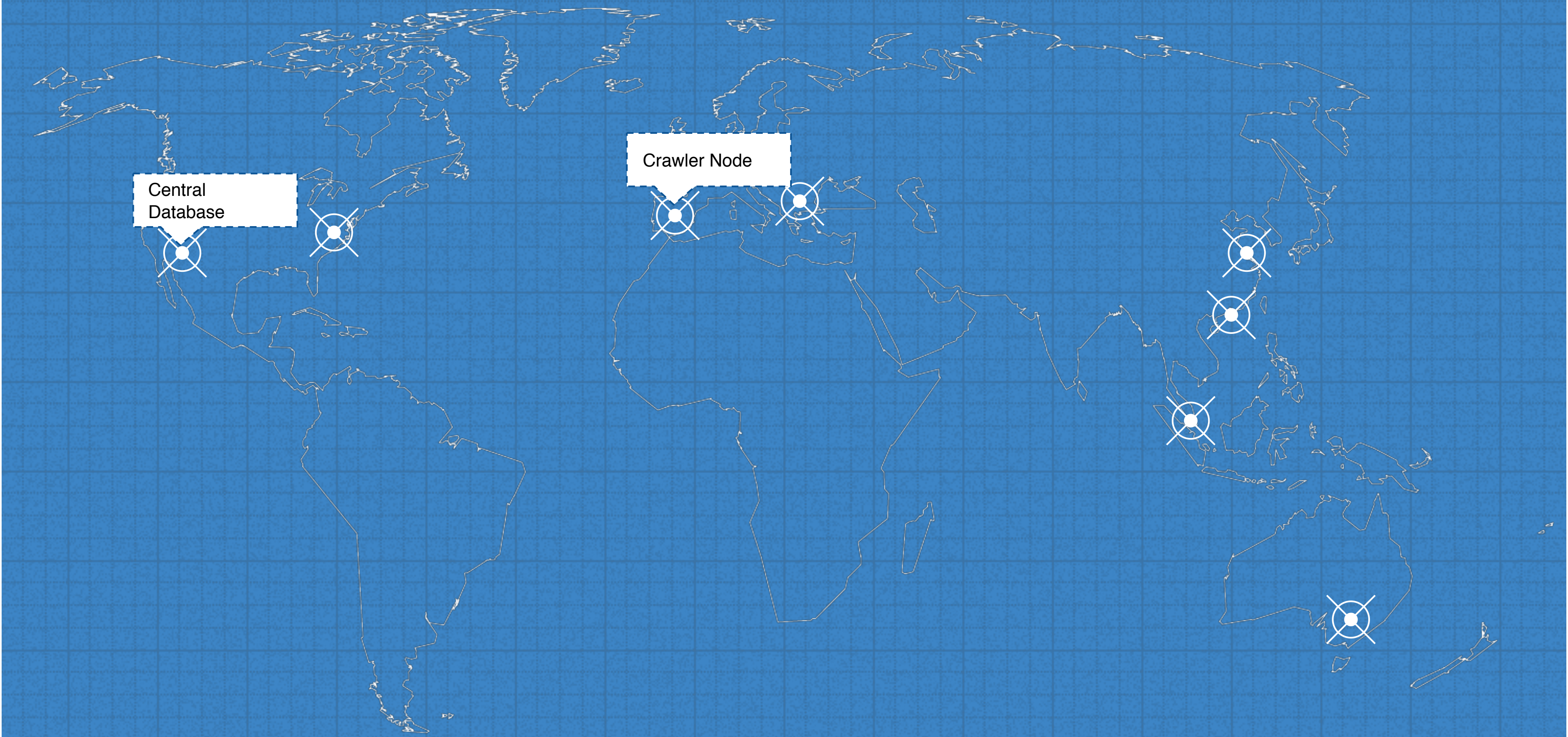
Website Database

Crawler

Platform Backend

Message Queue

Distributed System



TECH STACK

Backend:

- Flask(Python)

Frontend:

- React

Database:

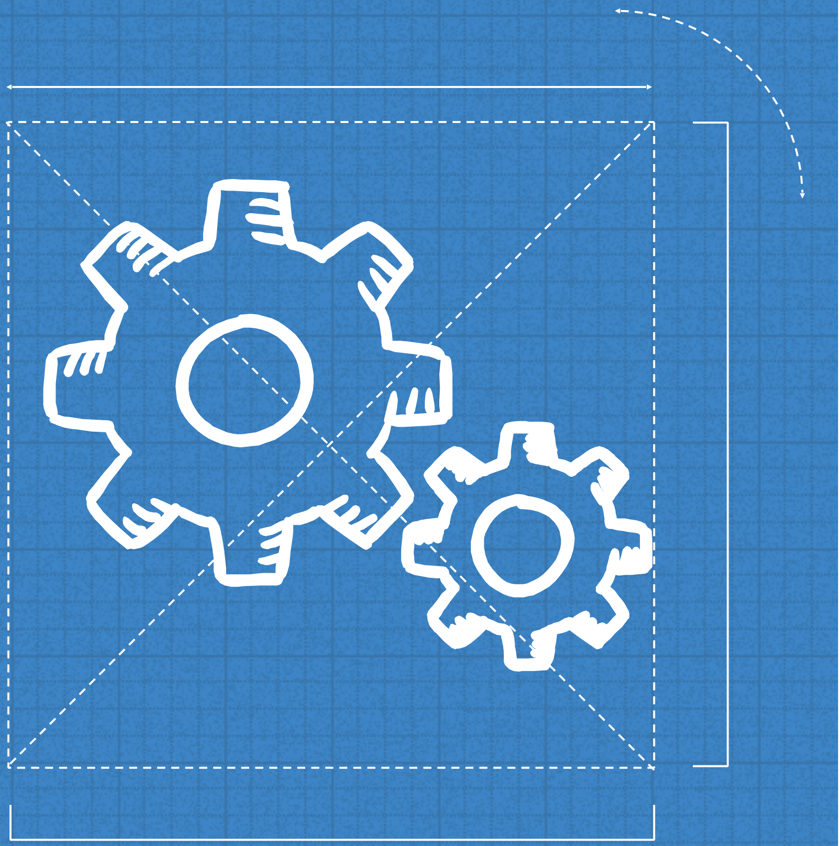
- MongoDB, MySQL

MPI:

- RabbitMQ

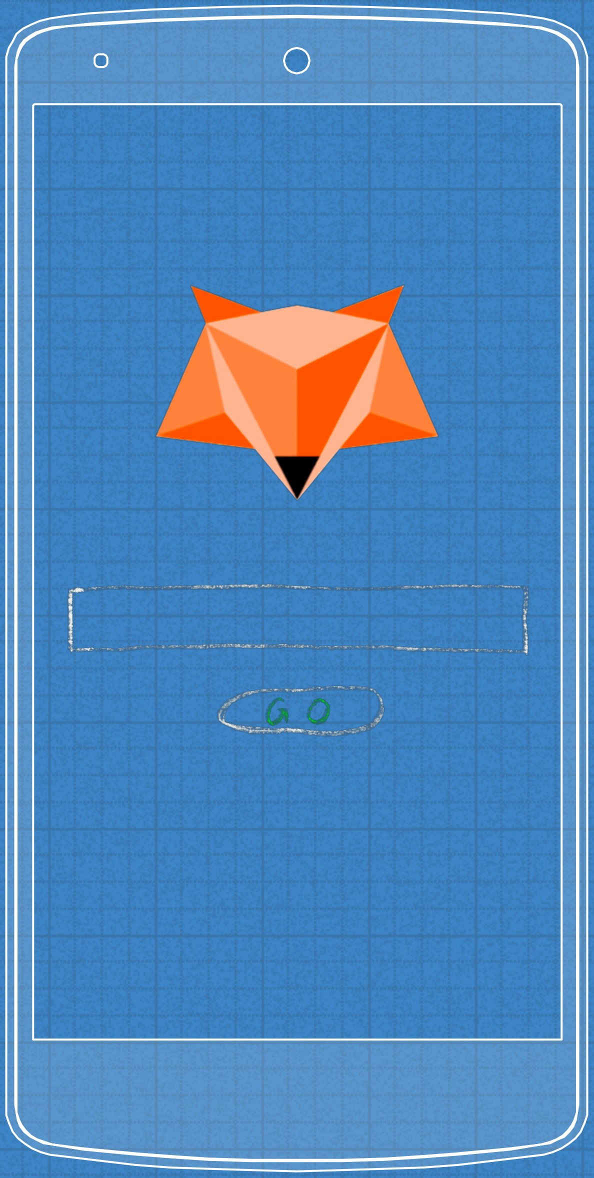
Scheduler:

- Celery(Python)



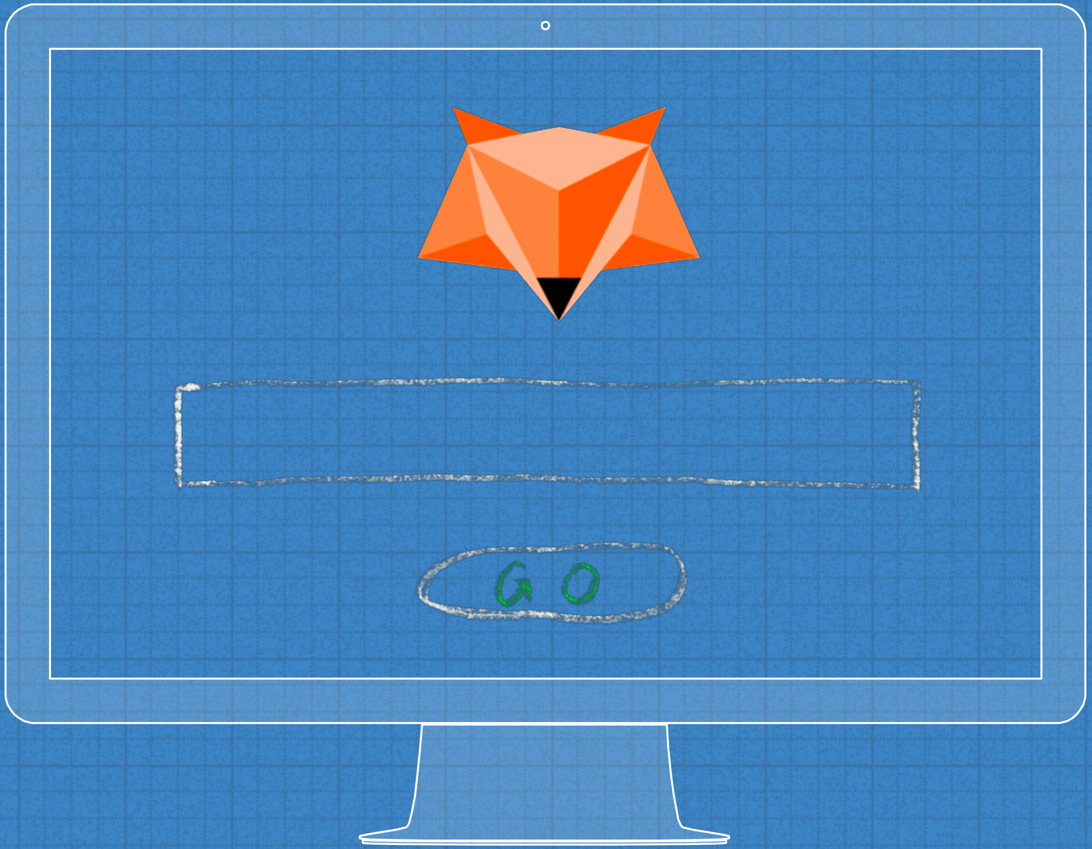
MOBILE PLATFORM

A frontend for normal viewers, designed for mobile devices resolution(375x667).



DESKTOP PLATFORM

A frontend for normal viewers & Website Owner, designed for prevalent devices resolution(1920x1080).



Thanks!

ANY QUESTIONS?