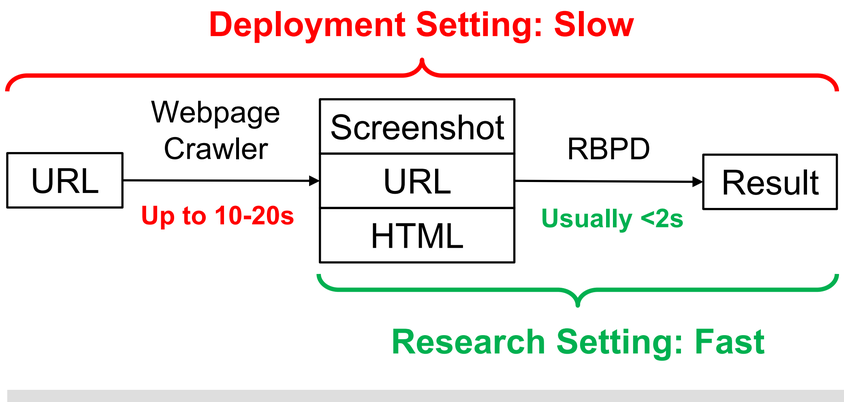
Demo Track

PhishIntel: Toward Practical Deployment of Reference-Based Phishing Detection

Yuexin Li, Hiok Kuek Tan, Qiaoran Meng, Mei Lin Lock, Tri Cao, Shumin Deng, Nay Oo, Hoon Wei Lim, Bryan Hooi

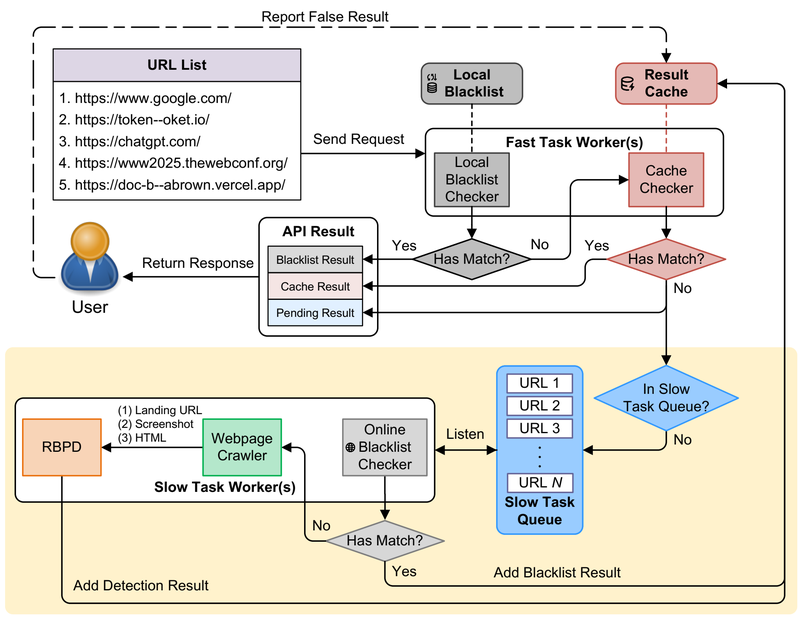
Motivation



Deployment Challenges of Reference-Based Phishing Detectors (RBPDs)

- RBPDs, such as Phishpedia (*USENIX Security* 2021), PhishIntention (*USENIX Security* 2022), KPD (*USENIX Security* 2024) enable fast phishing detection via visual/textual analysis.
- However, necessary inputs, including screenshots and HTML, are often unavailable; only URLs are presented in practice (e.g., phishing URLs in emails).
- Integrating webpage crawlers to retrieve missing input data introduces **substantial runtime latency**, hindering real-time deployment.

PhishIntel: A Deployment-Ready Phishing Detection System



An overview of PhishIntel

Fast-Slow Task Architecture

Fast Task:

- Checks the input URL against local blacklists and result cache. If a match is found, a detection result will be immediately returned.

Slow Task Queue:

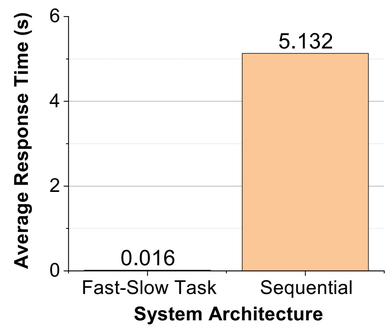
- Stores the URLs requiring slow task analysis (no fast task match).

Slow Task:

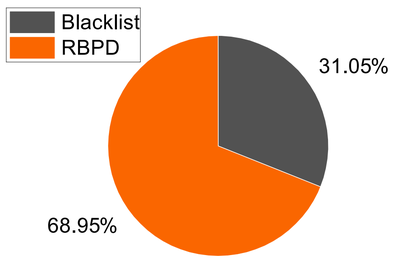
- Retrieves URLs from the Slow Task Queue to conduct in-depth phishing analysis, including online blacklist verification, webpage crawling and RBPD analysis.

Key Features

1. Instant response at user end.
2. Efficient URL filtering while retaining robust zero-day phishing detection capability.
3. Parallel processing of user URL requests.

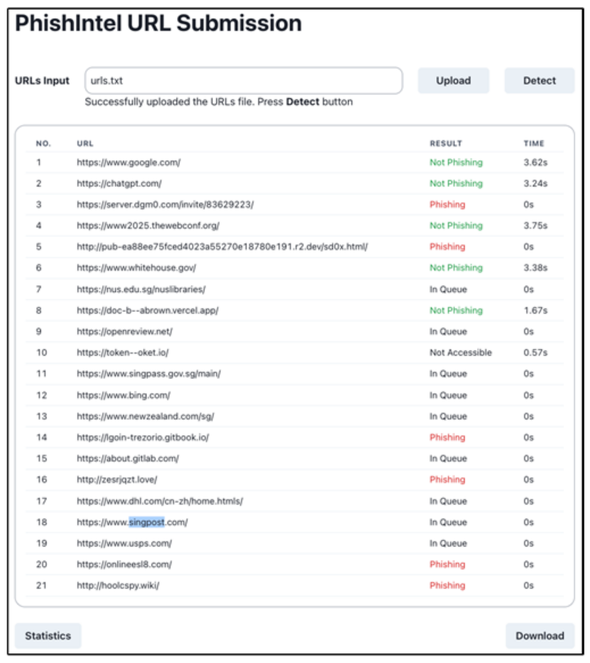


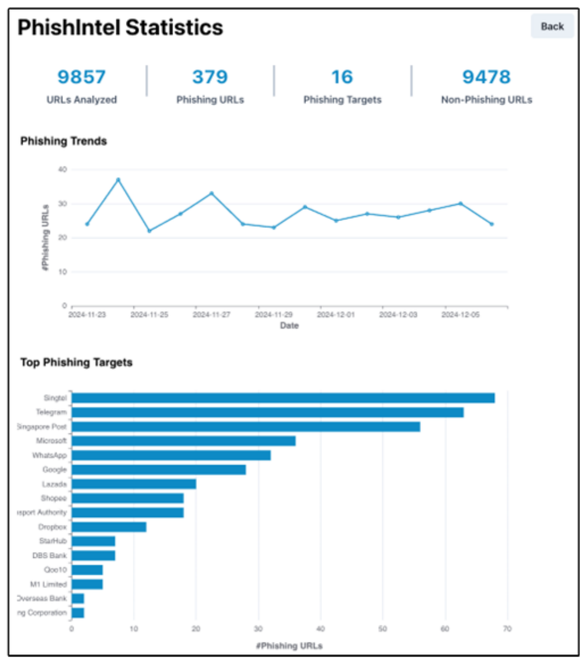
Comparison of the average response time with different system architectures.



Distribution of the phishing reports from blacklist and RBPD.

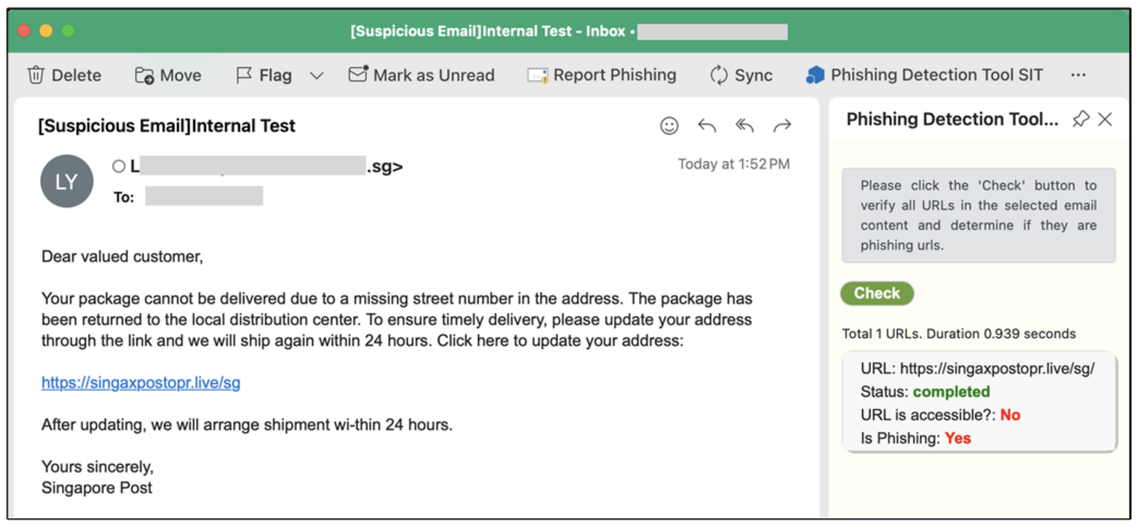
Applications





1. Phishing Intelligence Platform

- Users submit a .txt file with a list of URLs via the UPLOAD button, and trigger phishing detection via the DETECT button.
- A dashboard page visualizes phishing detection statistics derived from the result cache.



2. Phishing Email Detection Plugin

- When users encounter a suspicious email, they can click the button in this plugin to report for analysis.
- The plugin will extract all the URLs in the selected email as a list and send it to PhishIntel for phishing URL detection.

Our Phishing Research

KnowPhish
USENIX Security 2024

PhishAgent
AAAI 2025
(Oral Presentation)

PhishIntel
WWW 2025
(Demo Track)

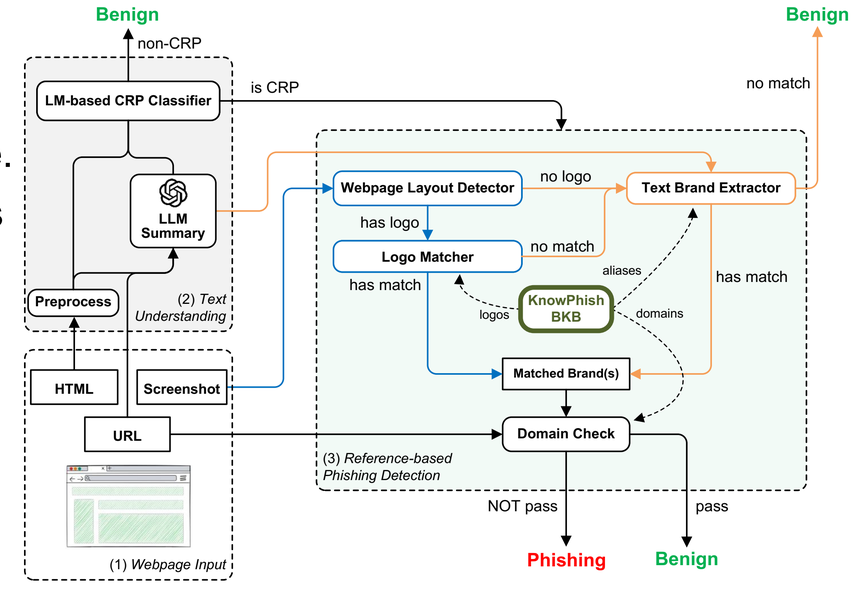
Additional Details

PhishIntel utilizes KPD+KnowPhish (*USENIX Security* 2024) as its RBPD backend.

- KnowPhish is a large-scale brand knowledge base, while KPD is a multimodal phishing detector backbone.
- KPD+KnowPhish detects the most phishing webpages both visually and textually, surpassing previous SoTA RBPDs in a Singapore-based field study.

Detector	BKB	#P	#TP↑	Precision↑	Time↓
Phishpedia	Original	54	17	31.48	0.16s
	DynaPhish	583	481	82.67	5.98s
	KnowPhish	353	333	94.33	0.16s
PhishIntention	Original	25	8	32.00	0.18s
	DynaPhish	163	140	85.89	5.91s
	KnowPhish	138	133	96.37	0.19s
KPD	DynaPhish	628	581	92.52	7.83s
	KnowPhish	699	681	97.42	1.64s

Phishing detection performance of different RBPDs in the SG field Study



An overview of our RBPD backend KPD+KnowPhish