UNIVERSITY

OF TRIESTE

Department of Engineering and Architecture

Bachelor's Degree in Electronic and Computer Engineering

Summary of *"Phishing in the Free Waters: A Study of Phishing Attacks Created using Free Website Building Services"*

Student:

Francesca Craievich

Supervisor:

Alberto Bartoli

A.A. 2023/2024

Index

1. The unique general topic of the proposed article

The article *"Phishing in the Free Waters: A Study of Phishing Attacks Created using Free Website Building Services"* introduces **FreePhish**, a framework designed to identify and analyse phishing sites created using Free Website Builders (FWBs). A **Free Website Builder** is an online tool or platform that allows users to create and publish websites at no cost, without needing to know programming languages or possess advanced technical skills. Most free website builders use a drag-and-drop interface, enabling users to easily select elements such as text and images and place them on the page. Some website builders provide a free subdomain as part of the package, such as "yourname.builder.com." Additionally, they offer free hosting, meaning that the created website is hosted on the builder provider's servers, and they include basic SEO (Search Engine Optimization) tools to help the site be better indexed by search engines.

The proposed FreePhish framework helps to automatically identify phishing attacks created with FWBs and shared on social media platforms like Twitter and Facebook, monitors the response of anti-phishing entities to these attacks, and reports them for removal.

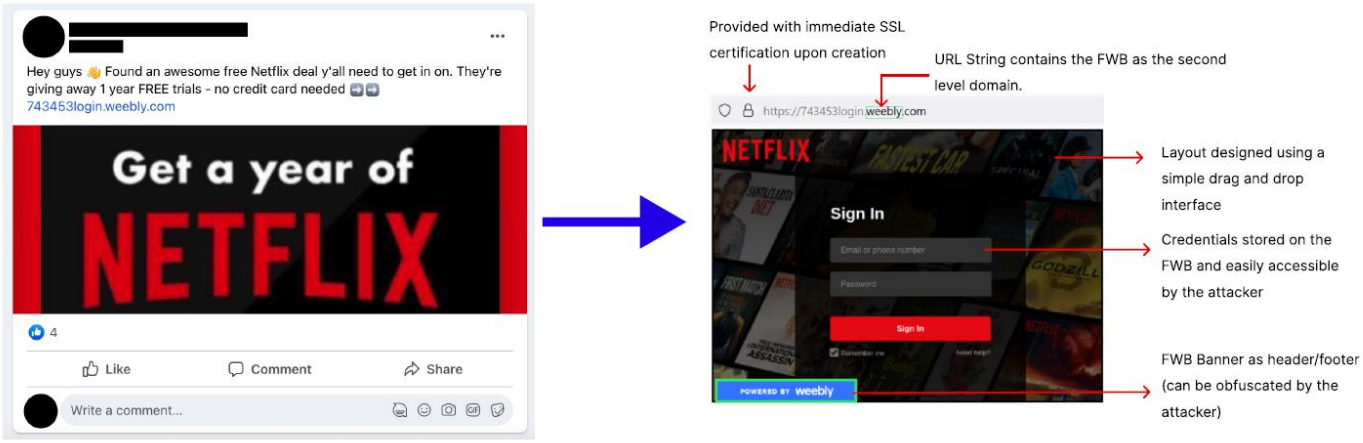

Figure 1: Typical phishing attack

2. Description of the specific problem addressed by FreePhish

Attackers are increasingly exploiting Free Web Builders (FWBs) to conduct malicious activities, taking advantage of their features that facilitate such operations. To demonstrate this trend, a total of 4.5 million URLs were collected through the official APIs of Twitter and Meta's CrowdTangle. Among these, 3.1 million URLs were obtained from Twitter and 1.4 million from Facebook, which included second-level domains (e.g., mywebsite.000webhost.com, where 000webhost functions as a second-level domain) distinct within their URL strings from January 2020 to August 2022. The focus on second-level URLs was driven by the intention to analyse websites created using FWB, as these are usually associated with second-level domains. The collected data were further corroborated by in-depth studies conducted by Interisle between 2020 and 2023.[1]

The URLs were then analysed using VirusTotal, a service that aggregates detection scores from 80 different anti-phishing tools. URLs with two or more detections were labelled as phishing. They identified 25.2K phishing URLs (16.3K from Twitter and 8.9K from Facebook) that utilized 17 free website builder services. Hereafter, these 25.2K URLs will be referred to in the document as the *initial dataset* or *D1*.

To better understand the characteristics that make phishing attacks created with FWBs particularly advantageous for attackers, a random sample of 5K URLs from Dataset D1 was closely examined. Two university students specializing in cybersecurity were selected as coders for this evaluation, which primarily assessed whether the URL and the appearance of the website attempted to mimic one of the 409 brands targeted by phishing attacks and if they contained text fields intended for collecting sensitive information.

Analysis of the data and the interfaces of the 17 FWB services reveals that these services have turned the tables in favour of the attackers, as they allow users to create websites for free without the need for continuous investment. Additionally, being subdomains of the FWB itself, they inherit the same domain age as the FWB, as recorded in the WHOIS database. For this reason, automated phishing detection measures that consider domain age as an important heuristic fail to detect them easily. Furthermore, FWBs require no coding experience and allow for the insertion of custom HTML code, which can be exploited by attackers to make the site appear more legitimate.

Another reason users are more likely to trust sites created with FWBs is that they generally come with high-credibility SSL certificates such as Extended Validation (EV) or Organization Validation (OV) and use top-level domains (TLDs) like ".com" or ".org". These sites are often difficult to discover because they contain the '`<no-index>`' tag in the source code, instructing search engines not to index the site, and obfuscated banner code that does not indicate that the site was created with an FWB. Of the randomly sampled 5K URLs, 4,656 were confirmed to be phishing.

[1] Interisle. Phishing Landscape 2020-2023. https://interisle.net

3. Internal function of FreePhish

FreePhish consists of five core components: **the streaming module, the preprocessing module, the classification module, the reporting module, and the analysis module.**

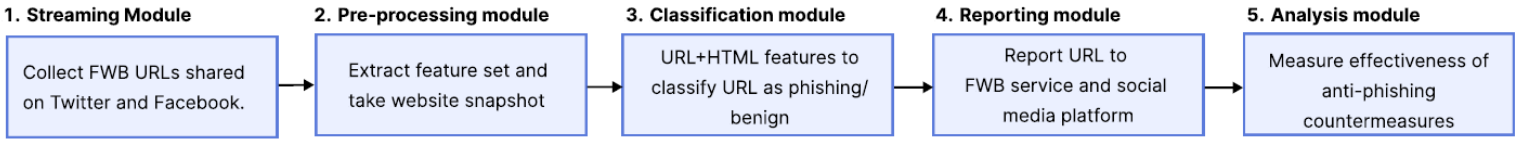

Figure 2: Overview of how FreePhish works

The streaming and pre-processing modules use the APIs of Twitter and CrowdTangle to collect new posts from Twitter and Facebook every 10 minutes. They use predefined lists of Facebook and Twitter pages and groups that are likely to share phishing links. They also use search queries with keywords related to phishing scams, and apply regular expressions to extract URLs from these posts. The pre-processing module store a complete snapshot of each site by extracting features based on the URL, HTML, and FWB, such as obfuscated banner code, credential fields, the presence of '`<no-index>`' tags, and more, which are then passed to the classification module.

The classification module was built using a ground-truth dataset on which four machine learning-based phishing detection models were tested to choose the best balance between efficiency and accuracy. Once one of the models was selected, they further refined it by adding or removing specific phishing-related features. For the ground-truth dataset, they used the 4,656 manually verified true positive URLs from D1, on which they tested VisualPhishNet, PhishIntention, StackModel, and URLNet. The models were tested on a system with an Intel Xeon W processor, 64 GB of RAM, and 2 NVIDIA RTX 2080i GPUs. They also selected and manually verified an equal number of true negative benign FWB-created URLs from D1 that were shared on Twitter (n=3,299) and Facebook (n=1,357).

Model	Accuracy	Precision	Recall	F1-score	Total Time Taken (sec)	Median Runtime (sec)
VisualPhishNet	0.76	0.78	0.72	0.75	14,802	5.1
PhishIntention	0.96	0.98	0.94	0.96	32,958	11.3
URLNet	0.68	0.70	0.67	0.68	4,471	1.9
Base StackModel	0.88	0.89	0.87	0.88	8099.4	2.4
Our Model	**0.97**	**0.96**	**0.97**	**0.96**	**8,658**	**2.8**

Table 1: With an F1 score of 0.96 and a median response of only 2.8 seconds, FreePhish is currently the most effective machine learning-based model for phishing detection. The F1 score is the harmonic mean between precision (% of correct results among those the model identified as positives) and recall (% of true positives out of total true positives).

From the table, it can be observed that PhishIntention achieved the best performance with a recall of 0.97. However, its complexity makes it significantly slower in classifying samples, with a median execution time of 11.3 seconds per URL**.**

As a result, the **StackModel** was chosen as it represents the best balance. Two of the features used by StackModel to detect phishing websites were replaced with more specific functions, such as *"Obfuscating FWB Footer"* and *"Preventing Indexing"*, which detect the presence of the

'<visibility: hidden>' tag to hide the FWB banner or the '<no-index>' tag that prevents search engines from indexing their URLs.

For training the StackModel architecture, the methodology of **Li et al**[2] was employed, which uses a two-layer stacking model that combines multiple ML models. In each iteration, the dataset (n = 4,656 phishing samples and 4,656 benign samples) is divided into 70% for the training set and 30% for the test set. This process continues until each base model, which are the ML models in the first layer of stacking, has predicted correctly.

The reporting module relies on the Python library Selenium to automate the submission of reports via the Chromium web browser to the respective FWBs and social media platforms. The URLs identified as phishing by the classification model are immediately sent including the full URL, a screenshot of the site, and the name of the targeted organization, after being approved by the cybersecurity office.

The analysis module is based on the assessment of anti-phishing entities, considering two indicators: coverage (percentage of URLs hosted by FWBs detected and removed within one week) and response time (the duration from the first appearance to removal). For each FWB phishing URL, it was checked whether it was present in four anti-phishing blocklists: Google Safe Browsing (GSB), PhishTank, OpenPhish, and APW eCrimeX.

They used VirusTotal to scan both FWB-based and self-hosted phishing URLs in their dataset every 10 minutes. To evaluate the domain removal, they checked whether the website was active every 10 minutes from when it first appeared in their dataset. Similarly, for Twitter and Facebook, using Twitter's API and Facebook's unique ID, they checked if the tweet/post had been deleted every 10 minutes.

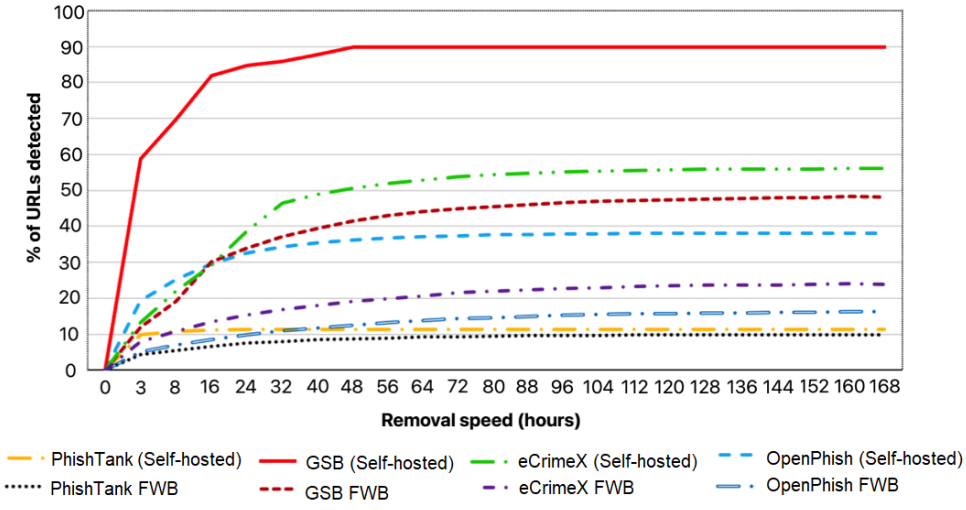

Figure 3: Coverage and speed of blocklists against FWB and self-hosted phishing attacks.

[2] Yukun Li, Zhenguo Yang, Xu Chen, Huaping Yuan, and Wenyin Liu. 2019. A stacking model using URL and HTML features for phishing webpage detection. *Future Generation Computer Systems* 94 (2019), 27-39.

4. Evalutation of FreePhish

They ran FreePhish for a period of six months, from November to May 2023, identifying 31.4K zero-day phishing attacks (19,724 URLs from Twitter and 11,681 from Facebook) created using free website builders. The analyses were also compared with self-hosted phishing attacks by running the StackModel during the same period and selecting a random sample of 31.4K URLs, ensuring that the sample distribution matched the distribution of FWB phishing attacks**.**

A longitudinal study was conducted to evaluate the effectiveness of 76 third-party anti-phishing tools on the dataset. The results reveal that approximately 50% of the FWB attacks spread through Twitter and Facebook had an average of four tool detections, while self-hosted phishing attacks had an average of 9 detections, indicating that FWB attacks are detected less frequently.

Method	FWB Phishing websites			Self-hosted Phishing Attacks		
	Coverage	Min/Max (hh:mm)	Median Speed (hh:mm)	Coverage	Min/Max	Median Speed
PhishTank	4.08%	0.10/116:13	07:11	17.4%	0:03/122:03	02:30
OpenPhish	11.70%	0:02/191:30	13:20	30.5%	0:01/146:18	02:21
GSB	18.44%	0:02/148:05	06:01	74.2%	0:01/146:26	00:51
eCrimeX	32.90%	0:07/137:43	08:54	47.9%	0:04/133:05	04:26
Social media Platform	23.06%	0:04/125:53	10:25	50.9%	0:07/114:23	03:41
Hosting domain	29.38%	0:19/158:25	09:43	77.50%	0:08/135:29	03:47

Table 2: Illustrates the capabilities of blocklists against both FWB and self-hosted phishing URLs. For example, GSB covered 18.4% of all FWB phishing URLs, with a median response time of 6 hours, far below its performance for self-hosted attacks with 74.2% coverage and median response of 51 minutes.

Given the low coverage of FWB phishing attacks by blocklists, the proactive removal of these websites by the domain registrar is crucial to prevent potential victims from visiting them. However, as illustrated in Table 2, only 29% of the websites were removed by the respective FWB with an average speed of 9 hours and 43 minutes.

Several factors influence the coverage and speed of removing phishing attacks by FWBs. To closely examine this issue, a random sample of 1K URLs from the dataset was analysed.

It was found that 539 URLs hosted on Google Sites contained a button that, when clicked, led to a phishing site on a different domain. This design avoids credential fields on the main website and does not directly share the phishing page, effectively evading detection by anti-phishing bots.

Furthermore, in 427 URLs on Google Sites and 473 URLs on Blogspot, attackers embedded an i-frame of a phishing site in the code of a benign website hosted on an FWB. This hidden i-frame is activated by clicking the button on the main website or loading alongside it.

Finally, 725 URLs on BlogSpot and 651 URLs on Google Sites were used to share malicious downloads hosted on third-party websites.

The combination of these tactics on these websites may further indicate the poor coverage of these attacks by anti-phishing entities.

Bibliographic Reference

Roy, S. S., Karanjit, U., & Nilizadeh, S. (2023). *Phishing in the Free Waters: A Study of Phishing Attacks Created using Free Website Building Services*. In *Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23), October 24–26, 2023, Montreal, QC, Canada*.

Site: https://doi.org/10.1145/3618257.3624812