PhishGNN: A Phishing Website Detection Framework using Graph Neural Networks

Tristan Bilot[1], Grégoire Geis[1] and Badis Hammi[1]
[1]*EPITA School of Engineering, France*
{*tristan.bilot, gregoire.geis, badis.hammi*}*@epita.fr*

Keywords: Phishing Detection, Graph Neural Networks, Deep Learning, Cybersecurity

Abstract: Because of the importance of the web in our daily lives, phishing attacks have been causing a significant damage to both individuals and organizations. Indeed, phishing attacks are today among the most widespread and serious threats to the web and its users. The main approaches deployed against such attacks are blacklists. However, the latter represents numerous drawbacks. In this paper, we introduce PhishGNN, a Deep Learning framework based on Graph Neural Networks, which leverages and uses the hyperlink graph structure of websites along with different other hand-designed features. The performance results obtained, demonstrate that PhishGNN outperforms state of the art results with a 99.7% prediction accuracy.

1 INTRODUCTION

In the era of the Internet, malicious URLs are a common threat to the Web users. Phishing aims at stealing sensitive information by fooling victims with falsified interfaces. In the case of phishing websites, attackers usually try to impersonate well-known and widely used services such as social media, banks and e-Commerce websites. Such spoofed websites are often built from the same code base as the original site, which could make them difficult to detect at first glance. Thankfully, numerous other indicators can be used to differentiate benign and phishing websites. For instance, most phishing URLs tend to be very long, with multiple sub-domains and special characters. Domains are often hosted on suspicious hosts and use Secure Socket Layer (SSL) certificates delivered by non-trusted authorities. Since the beginning of these attacks, numerous systems have been implemented to try to overcome them. Some of these implementations use traditional techniques such as blacklists or URL lexical features' analysis. However, blacklists suffer from multiple drawbacks like the need for human assistance to be updated and the lack of exhaustiveness. Furthermore, they cannot be used on unseen and hidden URLs. Other techniques leverage Machine Learning to train a model to classify websites based on a number of examples (Sahoo et al., 2017), (Benavides et al., 2020). However, in most approaches, the hyperlink structure of websites is not tackled.

In this paper we introduce PhishGNN, a framework that leverages and uses both hyperlink structural features along with every other feature that has been proven to be successful for phishing classification [1]. We also introduce features such as `is_same_domain` which are essential for differentiating two websites with the same structure. As many phishing websites redirect to legitimate ones, each link pointing to these websites has a different domain. However, on the legitimate website, these links are redirecting to the same domain, so the feature will be distinct in both cases and the model will learn how to differentiate them. We evaluated our approach through a real implementation. The performance results obtained demonstrate the efficiency and effectiveness of our approach in terms of detection accuracy and its capacity to outperform the existing detection approaches.

2 RELATED WORKS

The detection of phishing websites aims to classify whether websites are phishing or benign. Research in this area has increased sharply as the number of phishing websites has exploded in recent years. While advanced techniques have been proposed for this task, most solutions currently in production are based on blacklists (Sahoo et al., 2017). However, phishing

[1]https://archive.ics.uci.edu/ml/datasets/Phishing+Websites

websites become more and more complex and there is an urgent need for reliable and efficient techniques to detect them on demand, without human interaction.

2.1 Traditional Techniques

The most common technique used for the detection of phishing websites is the use of blacklists. However, this technique reveals numerous drawbacks, mainly: (1) it requires the curation of such a blacklist (and, therefore, is fallible to zero-day attacks and requires human involvement). (2) it requires the storage (space consumption) or the querying (time and computing resource consumption) of a blacklist. (3) crowd-sourced blacklists like PhishTank are centralized and lack transparency. The resources consumption problem is addressed by the Google Safe Browsing API [2], which is notably used in Chromium [3] and in Firefox as a fallback [4], by allowing clients to maintain a small local database which only contains truncated hashes of malicious URLs, and an online service which can be queried with a full hash when its truncated hash is found in the local database [5].

Prakash et al. (2010) also show that it is possible to build blacklists that, based on their current entries, can predict new entries with no human involvement. Cao et al. (2008) similarly build a list which automatically grows over time, though it differs in that it keeps track of legitimate websites (i.e. a whitelist).

Nonetheless, lists are flawed. Therefore, other techniques have been proposed to detect phishing using human-defined heuristics, designed after identifying inherent characteristics of known phishing websites.

These websites frequently rely on domain names to trick users into believing that they're visiting a website associated with a known, trusted entity. Since obtaining legitimate domains requires compromising their corresponding entity, phishing websites often use patterns in the URL to make them look like legitimate domains, while being subtly different. This can be done by confusing users with slightly different names (e.g. targeting "foobar.com" using the domain name "foo-bar.com"), by using subdomains of trusted entities (e.g. "foobar.example.com" [6]) or by including keywords related to the trusted entity in the path section of the URL (e.g. "example.com/foobar" (Teraguchi and Mitchell, 2004)).

Other lexical features derived from the URL can be useful. Sonowal and Kuppusamy (2020) suggest that having symbols such as "-" and "@", or having more than three dots in the domain name is suspicious, and considers long URLs suspicious as well because they make it harder for users to read the significant part of the URL.

Content features can also be significant, even with simple heuristics. Teraguchi and Mitchell (2004) can detect patterns such as similar-looking domains or links that point to an URL different from what they display to the user (e.g. `<a href="phishingsite.com">example.com</a>`). Sonowal and Kuppusamy (2020) assign lower legitimacy scores to web pages that have low accessibility scores and to those whose lexical signature (computed using the most frequent tokens in the page) do not appear in the first results of search engines.

Zhang et al. (2007) successfully consider older domains as more legitimate to identify phishing domain. However, the Anti-Phishing Working Group (APWG) noted in the 2016 APWG Global Phishing Report [7] that some attackers are starting to age domains before using them for attacks. Zhang et al. (2007) also use search engines and website rankings to automatically trust well-known websites. Although these approaches provide better accuracy, they rely on external services which slow down the classification of pages.

Some studies (Lakshmi and Vijaya, 2012) assume that legitimate websites are protected by Transport Layer Security protocol (TLS) and that phishing websites are not (because the issuer Certificate Authority (CA) must provide numerous verifications before providing a certificate). Nonetheless, this assumption no longer holds true because most phishing websites are now also protected by TLS (82% in 2021 [8]). Despite this, new techniques exist to assess the legitimacy of TLS certificates (Sakurai et al., 2020).

Phishing websites can protect themselves against content-based phishing detection by obfuscating the HTML content of their pages, or by using images instead of actual text. To counter this obfuscation, researchers have used image snapshots of suspicious pages to extract text content using optical character recognition (Dunlop et al., 2010), to determine whether the suspicious page looks like known, protected web pages (Wenyin et al., 2005), (Afroz and

[2] https://developers.google.com/safe-browsing/v4

[3] https://www.chromium.org/developers/design-documents/safebrowsing/

[4] https://wiki.mozilla.org/Security/Safe_Browsing

[5] https://developers.google.com/safe-browsing/v4/urls-hashing

[6] https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf

[7] https://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

[8] https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf

Greenstadt, 2009), or to look up whether the suspicious page used logos that are typically associated with other domains (Wang et al., 2011).

Finally, it has been shown that using combinations of different techniques leads to more accurate results (Sonowal and Kuppusamy, 2020), (Zhang et al., 2007).

2.2 Machine Learning Techniques

Machine Learning (ML) and Deep Learning (DL) has known a real boom during the last decade and has been widely used in the phishing classification task (Sahoo et al., 2017), (Benavides et al., 2020). When using such techniques, the first step is usually to extract a set of features from the URL. Although Deep Learning models have the ability to learn features by themselves from raw data, it is challenging to exploit them directly because a website is not only defined by its raw HTML content. Many useful features can be extracted by hand from the website's URL in order to build a more powerful and robust model. Deep Learning can be used on top of the features to let the model learn other kinds of representations that could improve the classification accuracy. These features can be divided in three classes: lexical, content and domain features.

Lexical features: features that could be extracted from the URL as a string. It is possible to extract efficient and meaningful features from the raw URL, like the URL length, the entropy, the number of special characters, the number of subdomains, and so on. Most Machine Learning phishing detection techniques highly rely on lexical features.

Content features: features related to the HTML content of the web page. Such features are obtained by fetching the DOM of the pages and then processing it to extract useful information like the number of anchors, the presence of a form, the number of Javascript imports, and so on. However, this feature extraction is more resource intensive.

Domain features: features are obtained from the domain name extracted from the URL. By requesting that domain, it is possible to extract features from the underlying server such as its location, the connection speed, "WHOIS" information, and so on. Another useful set of features that could be extracted from domain is the Secure Socket Layer (SSL) certificate, where we can discover the domain age, its expiration date, and whether it is delivered by a reliable authority or not. Domain features are known to be very expensive to extract but can lead to better predictions.

According to Sahoo et al. (2017) content-based and lexical-based features are mostly used in Machine Learning techniques, compared to host-based features, due to the extraction complexity of this one.

Most state of the art approaches for phishing classification are url-based. That is, they focus on the extraction of useful features directly from the raw URL. Some studies use traditional Machine Learning with hand-crafted features to make predictions (Abu-Nimeh et al., 2007), (Jain and Gupta, 2018), (Adeyemo et al., 2020), while others prefer using Deep Learning to let the model learn the features by its own (Sahoo et al., 2017). Using Deep Learning methods has the benefit to avoid human-assisted feature engineering and thus do not require the assistance of domain experts. Thanks to these benefits, numerous recent studies (Benavides et al., 2020) apply Deep Learning to URL classification. URL-based classification is a key process in the overall phishing classification task. This is due to the numerous lexical features possible to extract from a raw URL string.

Saxe and Berlin (2017) proposed eXpose, a solution based on a Convolutional Neural Network (CNN) (LeCun et al., 1995), where convolutions are applied to the URL at character-level to the raw URL (Zhang et al., 2015). The convolutions are used to find patterns between characters that could lead to interesting hidden features.

URLNet (Le et al., 2018) is a framework where a character-level CNN is used in combination with a word-level CNN. It is stated that using word-level features along with character-level features achieve better results for the URL classification task.

Some other methods use CNNs combined with Long Short-Term Memory (LSTM). Yu et al. (2018) detects algorithmically-generated domain names (DGA), and Yang et al. (2019) achieve 98.99% accuracy on URL classification using a preliminary classification based on URL features. However, the proposed method does not take in consideration domain features, which have been proven to be very efficient in the phishing classification task.

More recent studies take profit of the Transformer model and the attention mechanism to give appropriate weights for each feature and thus grant more attention to the most important ones (Maneriker et al., 2021), (Yuan et al., 2021).

Other techniques fetch domain information and scrap the HTML content of web pages to extract domain and content features. For example, Niakanlahiji et al. (2018) relies on a large number of features directly fetched from server, DNS and WHOIS.

Traditional Machine Learning models such as Random Forest, AdaBoost and kNN are then trained on these features to reach an accuracy of 95.4%. This study shows than Random Forest achieves better performance than other compared models. HTMLPhish (Opara et al., 2020), on the other hand, takes profit of CNNs to learn the semantic dependencies in the textual content of the raw HTML page. Using this architecture, they achieve 93% accuracy with no feature engineering required.

To the best of our knowledge, the sole application of Graph Neural Networks to phishing detection is based on the HTML structure of the website (Ouyang and Zhang, 2021). In this approach, a graph is built from the HTML DOM and a GNN is fed with this graph. At each GNN layer, every feature node aggregates the features of their neighboring nodes, resulting in node embeddings containing the overall graph information. Downstream classification models can then be used to predict based on these embeddings. However, this method only relies on the HTML content, which could be easily stolen from benign websites in order to build prefect website copies. This method could thus be easily bypassed by cloning the HTML structure of legitimate websites.

Unlike previous approaches, our solution takes advantage of the internal links structure of the website, along with the traditional features that led to successful results as shown in previous papers. By analysing many phishing websites, we figured out that most of them use similar "href" patterns in <a>, <form>and <iframe>tags. These links are usually self-loops anchors (URLs starting by #) or outgoing links to external domains (usually pointing to a legitimate website like a bank or a social media). Such patterns are useful for phishing classification because a neural network can be trained to learn how to distinguish websites with different structures. Malicious websites could hardly bypass this detection system because most of the outgoing links present on these websites redirect to external websites from other domain names in order to fool victims by persuading them that the website is legitimate.

3 PROPOSED APPROACH

3.1 Graph Neural Networks

Graph Neural Networks (GNNs) represent a type of neural networks that takes graph data as input. Unlike other neural network architectures, GNNs can handle non-euclidean data with complex relations between objects. Most GNNs follow the message-passing framework (MPNN) (Gilmer et al., 2017) and can be considered as a generalization of convolutional neural networks (CNN) for graphs. This message-passing algorithm takes as input a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with n nodes $v_i \in \mathcal{V}$ and m edges $(v_i, v_j) \in \mathcal{E}$, where $\mathcal{G}$ could be directed or undirected. Each node and edge can store a vector of features, respectively named node and edge features. Generally, all this information is represented through three matrices:

- A: the graph-structure matrix, of shape $n \times n$ in the case of an adjacency matrix and $2 \times n$ for a CSR (Compressed Sparse Row) or COO (COOrdinates) sparse matrix
- X: the node features matrix of shape $n \times d$
- E: the edge features matrix of shape $m \times e$

where $n = |V|$, $m = |E|$, d and e are respectively the number of features per node and per edge.

The message passing framework consists of four steps, where steps 1 to 3 are implemented by one GNN layer and are repeated as many times as the number of layers. Step 4 is a final step that should be applied after passing through every GNN layers.

1. MESSAGE: every node creates a message based on its node features and sends it to all neighbors.
2. AGGREGATE: nodes aggregate the incoming messages from every neighbor by using an aggregation function.
3. UPDATE: the old features of a node are updated by merging them with new features aggregated, creating node embeddings.
4. READOUT: combines every node embeddings into a representation that could be used in downstream Machine Learning algorithms for prediction.

Every step is generally a function with learnable parameters, that is, weight matrices and activation functions are used in the computation of both steps. One GNN layer usually corresponds to the propagation of features within a 1-hop neighborhood, so stacking n GNN layers will result in node features propagating up to n distant nodes. In each of these layers, every node gathers its neighbors' features. However, increasing the number of GNN layers is at date not considered as efficient as for CNNs (Alon and Yahav, 2020). When multiple node aggregations occur in the graph, the information tends to smooth and be approximately the same in every feature node (Oono and Suzuki, 2019). This phenomenon, called feature smoothing, becomes more and more present as the number of graph layers increases. Moreover, across long distances, GNNs are susceptible to bottlenecks. That is, the information can grow exponentially when

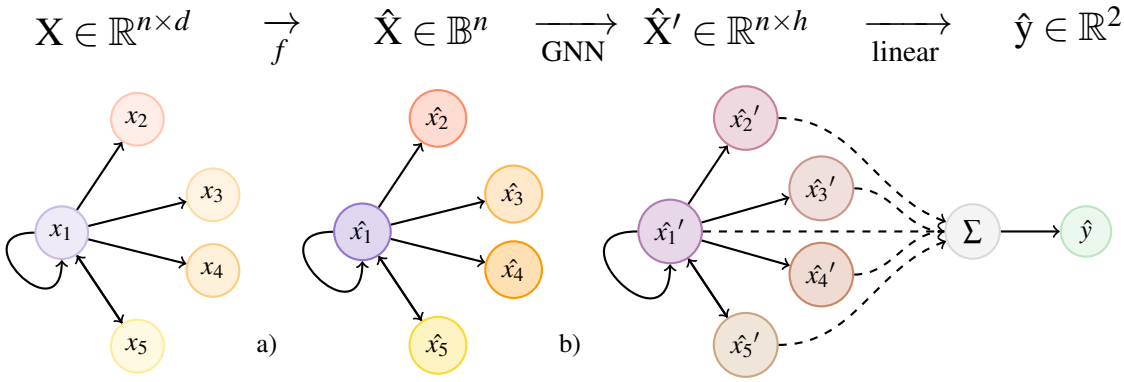

Figure 1: PhishGNN architecture comprises two steps: PRE-CLASSIFICATION (a) and MESSAGE-PASSING (b). Example using a graph with one root URL x_1 and 4 outgoing links $x_{2 \leq i \leq 5}$. The input feature matrix X is processed in these 2 steps to result in a prediction vector $\hat{y}$ containing the probability of the 2 classes.

multiple embeddings have to aggregate in a fixed-size embedding vector (Topping et al., 2021). This represents a main issue when there is a need to get long-distance information via message passing on the graph. Thankfully, in the phishing classification task with graphs, we are essentially interested in the 1-hop neighborhood of the classified URL, as the complexity for crawling n-hop neighborhoods grows exponentially with the number of URLs. For example, websites like wikipedia.org can be difficultly crawled with a depth greater than 1 as the feature extraction for thousands of nodes takes a huge amount of time.

3.2 PhishGNN

We propose PhishGNN, a framework for websites classification (phishing or benign) based on Graph Neural Networks. This framework can be considered as an additional layer to GNN architectures. Therefore, it can be easily plugged-in existing GNN implementations. We use graphs to leverage the hyperlink structure of websites. In the context of GNNs, we consider the task of phishing websites classification as a node classification task, where the node to classify is a given URL and the other nodes represent every possible link coming from that URL until a user-defined depth. From these links, it is possible to build a graph where nodes represent URLs, and edges are the links between URLs, extracted either from <a>, <form>or <iframe>tags. More precisely, the graph is a rooted graph where the root node is the website to classify (named root URL). The input dataset (fed to our classifier) contains a list of root URLs, mapping to a label: phishing or benign. For each URL in the dataset provided, a feature vector is extracted, as well as a vector of all URLs going from that root URL (children URLs). Features are also extracted for the children URLs. The feature vectors are used to build the feature matrix X. The children URLs are used to build the actual graph-structure matrix A.

In our approach, we suggest to train a model in a semi-supervised mode. The known labels are the actual root URLs and the unknown labels represent every child URL (i.e. we do not know if these URLs are phishing or not). Our contribution highly relies on the fact that knowing the label of every node around the root node makes that node much easier to classify. Given that labels are not known for every child URL, a classifier could be used to find an approximation for these labels. This classifier is trained on every supervised examples available in the dataset and is then used for inference on all other unsupervised examples. Afterwards, using a traditional GNN with message passing will gather information from classified nodes to build the embeddings. We use pooling methods such as add, max or mean on top of the embeddings to reduce graph dimension to a single node embedding. A linear layer is used as a final layer to make a prediction.

As Figure 1 shows, the architecture is divided into two steps:

(a) PRE-CLASSIFICATION: initially, the graph comprises n nodes, where each node $x_i (1 \leq i \leq n)$ is a vector of d features extracted from the corresponding i^{th} URL. x_1 is the root URL node and every node $x_i (1 < i \leq n)$ represent a link coming from x_1. At this first step, a binary classifier is used to predict in a semi-supervised mode whether a node is phishing or benign, for each feature node $x_i (1 \leq i \leq n)$. The classifier is a function $g : \mathbb{R}^d \rightarrow \mathbb{B}$, where $\mathbb{B}$ is the Boolean domain. After this step, the feature matrix X is transformed to a vector $\hat{\mathrm{X}}$ containing respectively zeroes and ones for legitimate and phishing predictions.

(b) MESSAGE-PASSING: the predictions are then passed through a traditional message passing GNN with h hidden layers, to propagate the information in the graph and learn node embeddings. This results into a matrix $\hat{X}'$ where each node is an embedding vector of size h. A pooling method is used to reduce the dimension of node embeddings to a single node of shape $1 \times h$. Finally, a dot product is applied between this node and a linear layer of shape $2 \times h$, resulting into a vector $\hat{y}$ containing the probability of belonging into each class: phishing or benign.

The graph-structure matrix A is stored in memory using the COO format, which requires only $O(|\mathcal{E}|)$ memory space, i.e. it grows linearly according to the number of edges. The feature matrix X uses $O(|\mathcal{V}| \times d)$ memory as it stores fixed-size feature vectors for each node.

The propagation rule of PhishGNN with a Graph Convolutional Networks (GCN) as MESSAGE-PASSING step is the same as the original GCN propagation rule:

$$f(H^{(l+1)}, A) = f(H^{(l)}, A) \tag{1}$$

$$f(H^{(l)}, A) = \sigma(\hat{D}^{\frac{-1}{2}}\hat{A}\hat{D}^{\frac{-1}{2}}H^{(l)}W^{(l)}) \tag{2}$$

where A is the adjacency matrix, $H^{(l)}$ is the propagation at layer l, σ is the ReLU non-linear activation function (Rectified Linear Unit), $W^{(l)}$ is a weight matrix at layer l, $\hat{A}$ is the adjacency matrix with self loops such that $\hat{A} = A + I$ (I is the identity matrix), and $\hat{D}$ is the diagonal matrix of $\hat{A}$.
However, instead of starting with $H^{(0)} = X$ in the original GCN, PhishGNN applies the PRE-CLASSIFICATION step to X such that $H^{(0)} = g(X)$, where g is a Random Forest prediction function.

4 PERFORMANCE EVALUATION

4.1 Evaluation Framework

To train the model and later evaluate arbitrary inputs, raw features related to a given URL must be obtained. Additionally, and unlike traditional classifiers operating on content features, PhishGNN must *crawl* web pages recursively to provide features for the pages referenced. Several existing crawlers were considered, but ultimately we implement a crawler specifically designed for PhishGNN with the following functionalities.

1. FINE-TUNED FEATURE EXTRACTION: feature extraction can be tailored to our use cases. Notably, workers can extract lexical features, content features, and domain features with no external dependencies (i.e. no sub-processes are needed during feature extraction).
2. ROBUSTNESS: `scraper` [9] (which uses Servo's [10] error-resilient HTML parser) is used for parsing and browsing HTML trees. `rust-url` [11] (similarly used by Servo) is used for parsing URLs, and `addr` [12] (which uses Mozilla's Public Suffix List [13]) is used for parsing domain names. `rustls` [14] is used with `webpki-roots` [15] for establishing safe TLS connections and rejecting invalid TLS certificates with sane defaults. Pages that take more than 10 seconds to read, or that are over than 1 MiB, or that lead to more than 10 redirects are dropped.
3. CONCURRENCY: multiple processes can operate on the same database at the same time, and each process can contain hundreds of workers which run in parallel (using OS threads) and concurrently (using asynchronous tasks).
4. DOMAIN-SPECIFICITY: multiple types of workers are available; *core* workers process pending URLs, extracting lexical and content features. *Domain* workers process pending domains, extracting domain features. This separation allows each domain to be processed only once, no matter how many pages are hosted on it.
5. EXTERNAL STORAGE: the processing queue lives entirely on a database separate from the workers.

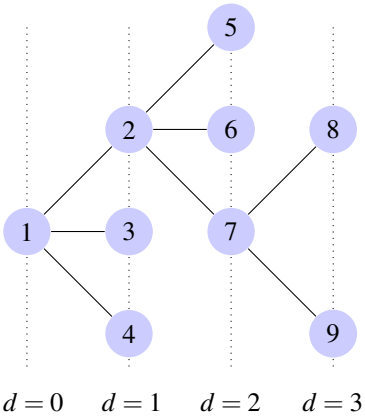

Figure 2: Crawling depth, noted as d. Node 1 is the root URL of depth 0, nodes 2, 3 and 4 are nodes of depth 1, etc.

[9] https://crates.io/crates/scraper
[10] https://servo.org/
[11] https://crates.io/crates/url
[12] https://crates.io/crates/addr
[13] https://publicsuffix.org/
[14] https://crates.io/crates/rustls
[15] https://crates.io/crates/webpki-roots

This enables distributed workers to be stopped or resumed at will, and direct interaction with the database to enqueue new pages or to monitor progress.

Crawling websites can be a heavy and time-consuming task. That's why it is mandatory to specify to the crawler when to stop the recursion. In Figure 2, we explain how the crawling *depth* works: a value determining how deep the crawler should go when iterating over the children of each web page. In this study, we have set the crawling depth to 1 (that is, both pages of depth 0 and 1 are crawled for their features), because using greater depth results in huge times for feature extraction. We classify the most important features extracted by the crawler (before the post-processing) as follows.

1. LEXICAL FEATURES: `is_https` (is the URL scheme "https"), `is_ip_address` (is the domain an IP address in any form), `domain_length` (length of the domain name, including subdomains and Top Level Domain (TLD)), `domain_depth` (number of dots in the domain name), `has_subdomain` (`domain_depth` $\geq$ 2), `dashes_count` (number of dash characters in the domain name), `has_at_symbol` (contains "@"), `is_same_domain` (false if the URL domain is not the same as the root URL).
2. CONTENT FEATURES: `is_valid_html` (false if the response body contains HTML parsing errors), `has_iframe` (true if an `<iframe>` tag is in the page document), `has_form_with_url` (true if a `<form>` element exists with a valid, static `src` attribute). References are added for `<a>` elements with valid (i.e. statically known and leading to a valid HTTP or HTTPS URL after resolution) `href` attributes, `<form>` elements with valid `action` attributes, and `<iframe>` elements with valid `src` attributes.
3. DOMAIN FEATURES: `is_cert_valid` (false if expired or rejected by `rustls`), `cert_country`, `cert_reliability` (computed using the duration of the certificate and whether its issuer is trusted), has_whois (false if WHOIS could not be resolved for the domain), `domain_age` (in seconds, between the last update date and the domain registry expiry date), `domain_end_period` (in, seconds between the date of the extraction and the domain registry expiry date).

Once features have been extracted by the crawler, they can be exported to a `csv` file which can then be read and pre-processed in Python. To better understand the underlying structure of each website, we have developed a tool to visualize every graph from the dataset[16]. In Figure 3, two crawled web pages, with totally different structures, are represented as graphs.

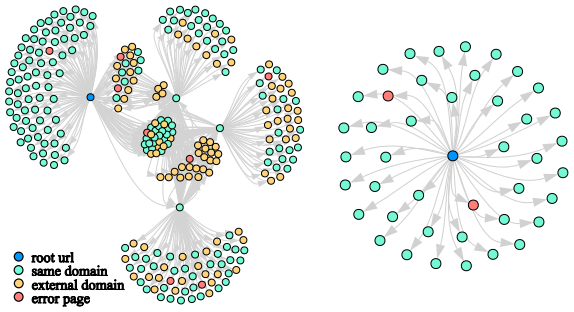

Figure 3: Graph representation of two websites after crawling with depth=1. Graph on the left contains multiple children URLs already crawled in previous iterations so their children are inserted in the graph as nodes of depth 2. Graph on the right contains children URLs never crawled before. Node in dark blue is the root URL, nodes in cyan and yellow are respectively URLs from the same domain and different domain, while red nodes are URLs returning an error code (HTTP status not in range 200-299).

4.2 Dataset

Finding a reliable public phishing dataset is fairly challenging because the lifetime of phishing websites is really short (few days or weeks). Hence, we have built a dataset based on around 30,000 malicious URLs, extracted from public phishing blacklists such as OpenPhish[17] or PhishTank[18]. However, most of these URLs redirect to 404 error pages as the corresponding websites are now out of service. The first filtering operation to apply on the dataset is thus to check that every website is responding with a successful HTTP code (i.e. in the range 200-299). This step has reduced the dataset size by 85%. Furthermore, some of the filtered URLs are labeled incorrectly. Indeed, totally legitimate websites like wikipedia.org or baidu.com are sometimes classified as phishing instead of benign. These incorrect classifications could lead to a biased model and therefore to incorrect predictions. To prevent this, we used the Google Safe Browsing API [19] in order to filter the dataset. Using this service on every URL from the dataset improves the reliability of each training example and brings a fairly better data quality but also removes a significant amount of data. This filtering step reduces the size of

[16]Tools, implementations and experiments developed and provided in this paper are available on GitHub https://github.com/TristanBilot/phishGNN.

[17]https://www.openphish.com/

[18]https://phishtank.org/

[19]https://developers.google.com/safe-browsing/v4

Model	Mean-Pooling	Max-Pooling	Add-Pooling	Time (s)
GIN	48±1.5	59±2.4	76±0.1	37.2
GAT	79±3.2	59±2.7	82±1.1	45.5
MemPooling	78±3.0	73±4.1	76±3.8	67.5
GCN_2	91±0.5	**93±0.2**	92±0.5	32.1
GCN_3	91±0.3	92±0.1	89±0.7	34.4
GraphSAGE	92±0.4	92±0.5	89±0.7	29.4
ClusterGCN	**93±0.3**	**93±0.6**	72±2.8	37.8

Figure 4: Model accuracy in % on test set for 10 epochs, for every implemented GNN. Each model is declined in three versions using multiple pooling methods (mean, max, add) as readout functions.

Model	Mean-Pooling	Max-Pooling	Add-Pooling	Time (s)
PhishGNN_GIN	52.4	53.2	71.2	23
PhishGNN_GAT	88.9	62.1	95.0	90
PhishGNN_MemPooling	75.8	99.2	98.0	23
PhishGNN_GCN_2	**99.7**	**99.7**	99.1	**20**
PhishGNN_GCN_3	99.7	99.7	99.2	22
PhishGNN_GraphSAGE	99.6	99.6	99.6	17
PhishGNN_ClusterGCN	99.7	99.7	97.2	24

Figure 5: Accuracy of PhishGNN framework on test set for 1 epoch using a Random Forest setting. $\text{PhishGNN}_{\text{GCN}_2}$, $\text{PhishGNN}_{\text{GCN}_3}$ and $\text{PhishGNN}_{\text{ClusterGCN}}$ achieve best results with 99.7% accuracy, where $\text{PhishGNN}_{\text{GCN}_2}$ is the fastest model for inference and training.

the dataset again by around 40% but has proven to be profitable. Furthermore, only websites containing at least a <form>, <input> or <textarea> tag are used for training. Indeed, we assume that phishing web pages usually request the user's personal information. A web page not containing such HTML tags is therefore not trying to steal any information.
Benign URLs are extracted from the Alexa top 1 million sites dataset [20]. The same filtering process is applied, except for the Safe Browsing API filter. We use approximately the same number of training examples in both classes in order to obtain a balanced dataset.

After the filtering steps, the overall dataset contains 4633 high quality URLs: 2300 benign and 2333 phishing, where 70% are used for training and 30% for testing. Graph matrices are built from the crawled URLs of the dataset. These graphs possess the following statistics: 90 average and 31 median nodes, ranging from 1 to 5185 nodes, 138 average and 45 median edges, ranging from 0 to 5214 edges.

4.3 Numerical Results and Discussion

4.3.1 Evaluation of Existing GNNs

A total of 7 well-known GNNs have been implemented and trained on the crawled dataset. Every model was implemented in Python using the PyTorch Geometric library. In this section, we describe the benchmarking performances of the models based on the raw features, without considering the PhishGNN implementation. For each GNN architecture, the network is trained for 10 epochs using Adam optimizer with a learning rate of 0.01, a weight decay of $1e{-}5$ and a batch size of 32. The loss is computed at each epoch using cross-entropy. Implemented models are GIN (Xu et al., 2018), GAT (Veličković et al., 2017), MemPooling (Ahmadi, 2020), GCN (Kipf and Welling, 2016), GraphSage (Hamilton et al., 2017) and ClusterGCN (Chiang et al., 2019). GCN_2 and GCN_3 are respectively implementations of GCN with 2 and 3 GCN layers. Training has been done on a NVIDIA Tesla K80 GPU using 16, 32 and 64 hidden neurons, where the setting with 32 hidden neurons gave the best accuracy. The obtained results are therefore based on models trained with hidden layers of size 32. Corresponding accuracies (mean $\pm$ standard deviation) and the average execution times are listed in Figure 4.

4.3.2 Evaluation of PhishGNN

In this section, we are interested in benchmarking PhishGNN framework with every GNN architecture implemented previously. Traditional Machine Learning techniques are also evaluated in order to find the best classifier to integrate with PhishGNN. As Figure 6 describes, most traditional Machine Learning methods achieve equivalent or even better results than the previous GNNs. Thereby, the Random Forest

[20] https://www.kaggle.com/datasets/cheedcheed/top1m

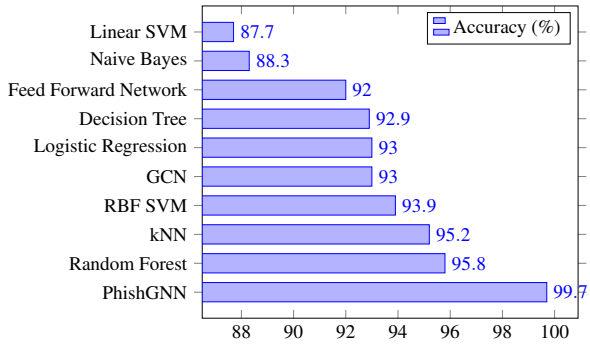

Figure 6: Classification accuracies between traditional Machine Learning methods, GCN and PhishGNN.

(i.e. the classifier with best accuracy) is chosen as the default classifier used in the PhishGNN architecture. By combining Random Forest predictions as PRE-CLASSIFICATION step and GCN_2 as MESSAGE-PASSING step, we outperform every other result by a large gap with an accuracy of 99.7%. The accuracy has been computed according to Equation 3:

$$Acc = \frac{C}{N} \tag{3}$$

where C is the number of correct predictions and N is the total number of predictions. A detailed analysis of true and false positives/negatives is demonstrated in Figure 7.

	Benign	Phishing	Total
Benign	688	3	691
Phishing	2	802	804
Total	690	805	1495

Figure 7: Confusion matrix for a test set of 1495 examples.

As Figure 5 shows, we achieve high scores with every pooling method in only one epoch. As predictions are already pre-computed in the PRE-CLASSIFICATION step, there is no need to train the GNN multiple times, as we want to propagate the information one time to obtain node embeddings.

To better understand the model predictions, node embeddings have been extracted directly after the pooling step and are plotted in Figure 8, using the T-distributed Stochastic Neighbor Embedding (TSNE) dimension reduction technique. Although the traditional GCN achieves great classification results, we see in embedding space that the model fails to delimit many nodes. However, thanks to the the PRE-CLASSIFICATION step in PhishGNN, node embeddings are more grouped and classes can be delimited by a straight line, which leads to a better classifications.

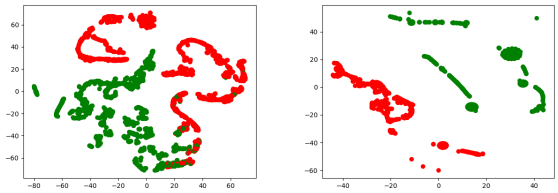

Figure 8: Embeddings of two models trained on our dataset. GCN_2 without PhishGNN framework (left) and with PhishGNN framework (right). Green: Benign; Red: Phishing

5 CONCLUSION AND FUTURE WORKS

To the best of our knowledge, we introduced the first Graph Neural Network framework applied to website hyperlink structure for the phishing classification task. Our experiments has shown that GNNs directly applied on the website graph structure is less efficient than traditional Machine Learning methods applied to features. However, by leveraging the semi-supervised structure of the graph, a classifier can be trained on supervised examples and make predictions on unsupervised ones. The semi-supervised predictions are then taken by a GNN as new input features and after message-passing, outperforms both traditional and Machine Learning techniques. The best accuracy has been achieved using a GCN combined with a Random Forest classifier. Furthermore, our approach is easily pluggable with any GNN architectures or other downstream classification methods. Hence, can be adjusted and improved in future works.

For future works we will focus on the establishment of a larger dataset, that contains more diverse examples. This dataset will be used in further research to improve benchmarking capabilities for phishing classification based on GNNs. We will also focus on improving the accuracy of our approach via leveraging edge features in the graph.

REFERENCES

Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. (2007). A comparison of machine learning techniques for phishing detection. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 60–69.

Adeyemo, V. E., Balogun, A. O., Mojeed, H. A., Akande, N. O., and Adewole, K. S. (2020). Ensemble-based logistic model trees for website phishing detection. In *International Conference on Advances in Cyber Security*, pages 627–641. Springer.

Afroz, S. and Greenstadt, R. (2009). Phishzoo: An automated web phishing detection approach based on profiling and fuzzy matching.

Ahmadi, A. H. K. (2020). *Memory-based graph networks*. PhD thesis, University of Toronto (Canada).

Alon, U. and Yahav, E. (2020). On the bottleneck of graph neural networks and its practical implications. *arXiv preprint arXiv:2006.05205*.

Benavides, E., Fuertes, W., Sanchez, S., and Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. *Developments and advances in defense and security*, pages 51–64.

Cao, Y., Han, W., and Le, Y. (2008). Anti-phishing based on automated individual white-list. In *Proceedings of the 4th ACM workshop on Digital identity management*, pages 51–60.

Chiang, W.-L., Liu, X., Si, S., Li, Y., Bengio, S., and Hsieh, C.-J. (2019). Cluster-gcn: An efficient algorithm for training deep and large graph convolutional networks. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 257–266.

Dunlop, M., Groat, S., and Shelly, D. (2010). Goldphish: Using images for content-based phishing analysis. In *2010 Fifth international conference on internet monitoring and protection*, pages 123–128. IEEE.

Gilmer, J., Schoenholz, S. S., Riley, P. F., Vinyals, O., and Dahl, G. E. (2017). Neural message passing for quantum chemistry. In *International conference on machine learning*, pages 1263–1272. PMLR.

Hamilton, W., Ying, Z., and Leskovec, J. (2017). Inductive representation learning on large graphs. *Advances in neural information processing systems*, 30.

Jain, A. K. and Gupta, B. (2018). Phish-safe: Url features-based phishing detection system using machine learning. In *Cyber Security*, pages 467–474. Springer.

Kipf, T. N. and Welling, M. (2016). Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907*.

Lakshmi, V. S. and Vijaya, M. (2012). Efficient prediction of phishing websites using supervised learning algorithms. *Procedia Engineering*, 30:798–805.

Le, H., Pham, Q., Sahoo, D., and Hoi, S. C. (2018). Urlnet: Learning a url representation with deep learning for malicious url detection. *arXiv preprint arXiv:1802.03162*.

LeCun, Y., Bengio, Y., et al. (1995). Convolutional networks for images, speech, and time series. *The handbook of brain theory and neural networks*, 3361(10):1995.

Maneriker, P., Stokes, J. W., Lazo, E. G., Carutasu, D., Tajaddodianfar, F., and Gururajan, A. (2021). Urltran: Improving phishing url detection using transformers. In *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)*, pages 197–204. IEEE.

Niakanlahiji, A., Chu, B.-T., and Al-Shaer, E. (2018). Phishmon: A machine learning framework for detecting phishing webpages. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 220–225. IEEE.

Oono, K. and Suzuki, T. (2019). Graph neural networks exponentially lose expressive power for node classification. *arXiv preprint arXiv:1905.10947*.

Opara, C., Wei, B., and Chen, Y. (2020). Htmlphish: enabling phishing web page detection by applying deep learning techniques on html analysis. In *2020 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE.

Ouyang, L. and Zhang, Y. (2021). Phishing web page detection with html-level graph neural network. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 952–958. IEEE.

Prakash, P., Kumar, M., Kompella, R. R., and Gupta, M. (2010). Phishnet: predictive blacklisting to detect phishing attacks. In *2010 Proceedings IEEE INFOCOM*, pages 1–5. IEEE.

Sahoo, D., Liu, C., and Hoi, S. C. (2017). Malicious url detection using machine learning: A survey. *arXiv preprint arXiv:1701.07179*.

Sakurai, Y., Watanabe, T., Okuda, T., Akiyama, M., and Mori, T. (2020). Discovering httpsified phishing websites using the tls certificates footprints. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 522–531. IEEE.

Saxe, J. and Berlin, K. (2017). expose: A character-level convolutional neural network with embeddings for detecting malicious urls, file paths and registry keys. *arXiv preprint arXiv:1702.08568*.

Sonowal, G. and Kuppusamy, K. (2020). Phidma–a phishing detection model with multi-filter approach. *Journal of King Saud University-Computer and Information Sciences*, 32(1):99–112.

Teraguchi, N. C. R. L. Y. and Mitchell, J. C. (2004). Client-side defense against web-based identity theft. *Computer Science Department, Stanford University. Available: http://crypto. stanford. edu/SpoofGuard/webspoof. pdf*.

Topping, J., Di Giovanni, F., Chamberlain, B. P., Dong, X., and Bronstein, M. M. (2021). Understanding over-squashing and bottlenecks on graphs via curvature. *arXiv preprint arXiv:2111.14522*.

Veličković, P., Cucurull, G., Casanova, A., Romero, A., Lio, P., and Bengio, Y. (2017). Graph attention networks. *arXiv preprint arXiv:1710.10903*.

Wang, G., Liu, H., Becerra, S., Wang, K., Belongie, S. J., Shacham, H., and Savage, S. (2011). *Verilogo: Proactive phishing detection via logo recognition*.

Wenyin, L., Huang, G., Xiaoyue, L., Min, Z., and Deng, X. (2005). Detection of phishing webpages based on visual similarity. In *Special interest tracks and posters of the 14th international conference on World Wide Web*, pages 1060–1061.

Xu, K., Hu, W., Leskovec, J., and Jegelka, S. (2018). How powerful are graph neural networks? *arXiv preprint arXiv:1810.00826*.

Yang, P., Zhao, G., and Zeng, P. (2019). Phishing website detection based on multidimensional features driven by deep learning. *IEEE access*, 7:15196–15209.

Yu, B., Pan, J., Hu, J., Nascimento, A., and De Cock, M. (2018). Character level based detection of dga domain names. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE.

Yuan, J., Liu, Y., and Yu, L. (2021). A novel approach for malicious url detection based on the joint model. *Security and Communication Networks*, 2021.

Zhang, X., Zhao, J., and LeCun, Y. (2015). Character-level convolutional networks for text classification. *Advances in neural information processing systems*, 28.

Zhang, Y., Hong, J. I., and Cranor, L. F. (2007). Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web*, pages 639–648.