Electronic Communications of the EASST
Volume 080 (2021)

Conference on Networked Systems 2021 (NetSys 2021)

Modular Platform for Detecting and Classifying Phishing Websites Using Cyber Threat Intelligence

Ahmed M. Elmisery and Mirela Sertovic

4 Pages

Guest Editors: Andreas Blenk, Mathias Fischer, Stefan Fischer, Horst Hellbrück, Oliver Hohlfeld, Andreas Kassler, Koojana Kuladinithi, Winfried Lamersdorf, Olaf Landsiedel, Andreas Timm-Giel, Alexey Vinel

ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Modular Platform for Detecting and Classifying Phishing Websites Using Cyber Threat Intelligence

Ahmed M. Elmisery[1], and Mirela Sertovic[2]

[1]amelmesiry@gmail.com
Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, UK

[2] msertovic@yahoo.com
Threat Defense Unit, Concept Tech Int. Ltd, Belfast, UK

Abstract: Phishing attacks are deceptive types of social engineering techniques that attackers use to imitate genuine websites in order to steal the login credentials and private data of the end-users. The continued success of these attacks is heavily attributed to the prolific adoption of online services and the lack of proper training to foster a security awareness mindset of online users. In addition to the financial and reputational damages caused by data breaches of individual users and businesses, cyber adversaries can further use the leaked data for various malicious purposes. In this work, a modular platform was introduced that facilitates accurate detection and automatic evaluation of websites visited by employees of a company or organization. The basis for this approach is a preceding website analysis, which is essential when hunting for potential threats from proxy logs. The platform contains three modules. Characterization of suspicious websites relies on a set of pre-defined features and a multi-stage threat intelligence technique, the functionality of which has been ascertained in initial tests on real data sets.

Keywords: Phishing, Threat intelligence, Cybersecurity, Malicious URL detection

1 Introduction

The widespread adoption of online services by public and private organizations facilitates conducting various business operations with their clients in an easy manner regardless of their physical location and time availability [Koufaris'02]. Conducting transactions and operations in this way has proven to be more convenient to most clients. However, there are serious risks associated with this model as demonstrated in [Lampe, Wenge, Müller, & Schaarschmidt'13].
Internet users face a variety of security threats while using online services, one of which is phishing attacks, where attackers use various tools and techniques to trick internet users into visiting malicious websites that mimic real ones to steal their login credentials and private data. The recent worldwide shutdown due to the novel coronavirus pandemic has forced millions, if not billions, to stay and work at home, attackers are finding this an incredible opportunity to look for new ways to commit cybercrime [Plachkinova'21]. In the latest report published in [AntiPhishing-Working-Group'21], January 2021 was a high in the trend of phishing attacks with an unprecedented 245,771 attacks in one month. Business e-mail compromise has caused aggregate losses in the billions of dollars, at large and small companies. Phishing attacks are frequently used as a vehicle for the rapid dissemination of malware and ransomware, where cyberattacks directed against a specific individual, organization, or company may rely on redirecting the victims to external malicious websites after receiving an email to evade anti-malware and anti-spam programs that stop spear-phishing emails containing malicious attachments at the email security gateway.

This paper introduces CTIP: " Cyber Threat Intelligence Platform". The purpose of CTIP is to build intelligence about web surfing activities, transforming raw proxy logs into substantial knowledge to uncover the suspicious websites visited by employees of a company or organization. This information proves valuable for long-term security posture management, in particular, for understanding what actually happened after a certain incident. CTIP enables a proper assessment and consistent recognition of known as well as unknown suspicious websites based on a multi-stage threat intelligence technique. Using a visual workflow for the entire process makes the platform more user-friendly. CTIP has its own infrastructure to automatically capture and analyze all visited websites within the perimeter of the enterprise network, making it easy to identify and investigate a potential threat in a timely manner. It should be possible to share the visual workflow of any multi-stage threat intelligence technique and replicate results, reducing the time required to triage and analyze data by prioritizing any visited suspicious websites. The proposed platform enables a typical monitoring infrastructure for the collection, storage, and analysis of proxy logs in a security posture management of an operational environment.

2 Related Work

Most of the literature deals with the problem of detecting suspicious websites using different methods and approaches. Signature-based detection is one of the widely used methods for the characterization of suspicious websites. as such, a database of blacklisted URLs is maintained to contain a list of malicious websites that were previously detected [Boddy'18]. Any newly requested website is matched against this database to determine if it has previously been flagged as malicious. The most common databases employed for this task are Google® Safe Browsing and PhishTank®. In principle, Signature-based detection usually fails to detect newly created malicious websites that have not been previously reported. More recent research has begun to use computational intelligence methods for the characterization of suspicious websites. as such, a set of common features relevant to malicious and genuine websites were elicited and then utilized for building classification models. The research work in [Corona et al.'17] trained support vector machines classifier on a multiple set of features. The experiment used an evaluation dataset containing 200 genuine and 325 suspicious websites. In [Ma, Saul, Savage, & Voelker'09] the authors utilized the properties of URL and domain name extracted from external sources to train naïve Bayes and linear regression classifiers to detect suspicious websites. In [Abdelhamid, Ayesh, & Thabtah'14] the authors created a set of 16 features derived from URL, content, and external sources, which was used to train some sort of multi-label classifier to recognize suspicious websites. A similar study was conducted in [Mohammad, Thabtah, & McCluskey'12], in which the authors designed a set of 30 features, which were categorized into four main features groups related to URL, abnormality, content, and the website domain. In [Rieck, Krueger, & Dewald'10], the authors developed Cujo as a web proxy component between a web client and a web service. Cujo intercepts and analyzes the raw data of a website before sending it to the web client. The solution in [Gastellier-Prevost, Granadillo, & Laurent'11] implemented an anti-phishing toolbar that utilizes 20 heuristics tests to analyze the properties of URLs and webpages. The evaluation results demonstrate that the combination of URL and HTML heuristics is an efficient way to distinguish websites. The growing number of proxy logs inevitably requires automatic models to efficiently detect, classify and share suspicious websites, which is also required for any threat hunting activities.

3 Methodology

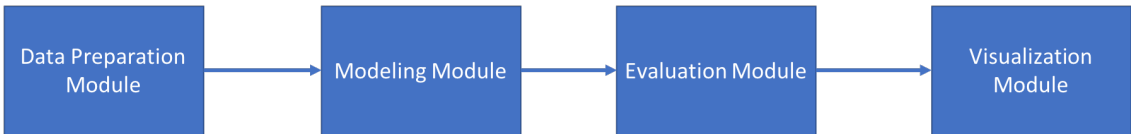

Figure 1: Multi-stage Threat Intelligence Workflow

The proposed multi-stage threat intelligence technique consists of four main modules, which are interconnected together. Specifically, these modules are data preparation, modeling, evaluation, and visualization. Figure 1 depicts the basic workflow between these modules. The raw web surfing is collected using browser-based open-source intelligence plugin, which allows large-scale harvesting of URLs and metadata from external sources. This will cover all the possible features that are required for the later stages. This data is provided to the **data preparation module** for filtering and pre-processing stages. The data preparation module continues to read all datasets, then filters the features into categories. Besides the properties of the URLs, metadata related to requested websites is analysed in relation to the content of web pages. Existing features are gathered and stored locally. Depending on the type, they can be stored as a separate value or combined with other sub-values to form a new feature set. In addition, if the correlations between the characteristics of these features are identified, the different categories are linked together. The results of this module are further processed using the **modeling module**. The robust features entries from different users are combined into the centralized log server, fed by pre-existing profiles that already exist for different websites, and form the basis for the modeling stage. Each logged feature is weighted statistically according to its importance and frequency in characterizing suspicious websites. The features deduced in this work are based on the phishing websites features [Mohammad et al.'12]. These features are utilized in the model building process, we implemented the C4.5 algorithm [Quinlan'93] to build a decision tree classifier based on a labeled data set using entropy. The overall result of the detection depends on the label assigned by the classifier to a new instance (recently requested website). With the proposed methodology, feature vectors of different categories can be assigned to each website. A chain of features can be a determinant for suspicious websites. The classification task is carried out using a decision tree classifier (rule-based tree), which is built in a top-down or general-to-specific manner based on the training stage. The generated model will then be used to perform the classification task on new instances. The process of building the model is initiated with a root node to label all the logged records. If the root node is enough to label all the instances, then the task is finished. Otherwise, more nodes and leaves are added to the tree recursively until all the instances belong to one of the existing classes. The **evaluation module** is responsible for evaluating the accuracy of the detection model, the convenient precision, and F-measure rates have been used as metrics. The number of misclassified websites along with the F-measure rate were used to evaluate the accuracy between the generated model and a baseline model. The two metrics TN (True Negatives) and TP (True Positives) respectively indicate the number of websites that were correctly identified as suspicious, and genuine. The results obtained from the evaluation module are passed to the **visualization module**, which is responsible for presenting the detection results in a human-readable form. The detailed information from the analysis of websites is stored in a machine-readable form, which can be used to further prioritize threat hunting activities.

4 Results and Discussion

This work presents a modular platform for detecting and classifying phishing websites using a multi-stage threat intelligence technique. The chosen approach offers a clear structure and comprehensive results. The approach is designed so that the statistically determined features of suspicious websites are scored higher than those of the original websites. Using CTIP, unknown suspicious websites can easily be detected. The proposed multi-stage threat intelligence technique is currently in the training and testing phases, TP rates (96%, 98%) were obtained on a real data set, by correctly identifying suspicious and genuine websites respectively, with an overall accuracy of 97% and more than 90% confidence. As shown in Figure 2, the developed cyber threat intelligence platform can be extended with various open-source intelligence extensions, daemons and services to ensure proper logging of web access traffic. It is planned to simulate a technical network of different nodes and to explore a covert cyberattack of APT on the infrastructure of this network. For this purpose, interfaces were developed in the modular platform. The final stage will utilize holistic techniques and field tests of the platform.

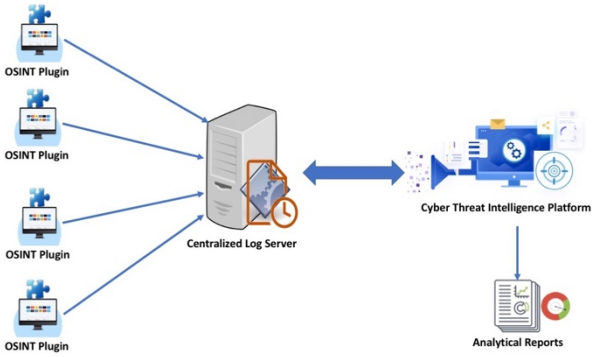

Figure 2: Schematic Structure of Cyber Threat Intelligence Platform

Bibliography

[Abdelhamid, N, Ayesh, A, & Thabtah, F2014] Abdelhamid, N, Ayesh, A, & Thabtah, F. (2014). Phishing detection based associative classification data mining. *Expert Systems with Applications, 41*(13), 5948-5959.

[AntiPhishing-Working-Group2021] AntiPhishing-Working-Group. (2021). *Phishing activity trends report*. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

[Boddy, M2018] Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. *Computer Fraud & Security, 2018*(11), 8-10.

[Corona, I, Biggio, B, Contini, M, Piras, L, Corda, R, Mereu, M, . . . Roli, FYear] Corona, I, Biggio, B, Contini, M, Piras, L, Corda, R, Mereu, M, . . . Roli, F. (2017). *Deltaphish: Detecting phishing webpages in compromised websites*. Paper presented at the European Symposium on Research in Computer Security.

[Gastellier-Prevost, S, Granadillo, GG, & Laurent, MYear] Gastellier-Prevost, S, Granadillo, GG, & Laurent, M. (2011). *Decisive heuristics to differentiate legitimate from phishing sites*. Paper presented at the 2011 Conference on Network and Information Systems Security.

[Koufaris, M2002] Koufaris, M. (2002). Applying the technology acceptance model and flow theory to online consumer behavior. *Information systems research, 13*(2), 205-223.

[Lampe, U, Wenge, O, Müller, A, & Schaarschmidt, RYear] Lampe, U, Wenge, O, Müller, A, & Schaarschmidt, R. (2013). *On the relevance of security risks for cloud adoption in the financial industry*. Paper presented at the AMCIS.

[Ma, J, Saul, LK, Savage, S, & Voelker, GMYear] Ma, J, Saul, LK, Savage, S, & Voelker, GM. (2009). *Beyond blacklists: Learning to detect malicious web sites from suspicious urls*. Paper presented at the Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining.

[Mohammad, RM, Thabtah, F, & McCluskey, LYear] Mohammad, RM, Thabtah, F, & McCluskey, L. (2012). *An assessment of features related to phishing websites using an automated technique*. Paper presented at the 2012 International Conference for Internet Technology and Secured Transactions.

[Plachkinova, M2021] Plachkinova, M. (2021). Exploring the shift from physical to cybercrime at the onset of the covid-19 pandemic. *International Journal of Cyber Forensics and Advanced Threat Investigations, 2*(1), 13. doi:10.46386/ijcfati.v2i1.29

[Quinlan, JR1993] Quinlan, JR. (1993). C 4.5: Programs for machine learning. *The Morgan Kaufmann Series in Machine Learning*.

[Rieck, K, Krueger, T, & Dewald, AYear] Rieck, K, Krueger, T, & Dewald, A. (2010). *Cujo: Efficient detection and prevention of drive-by-download attacks*. Paper presented at the Proceedings of the 26th Annual Computer Security Applications Conference.