КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.830
УДК 004.056.5:004.738.5:004.822

Бучик Сергій Степанович
доктор технічних наук, професор кафедри кібербезпеки та захисту інформації
Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0003-0892-3494
buchyk@knu.ua

Толстяк Маргарита Сергіївна
студентка кафедри кібербезпеки та захисту інформації
Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID ID: 0009-0007-9221-8187
tolstiakm@knu.ua

ДЕТЕКТУВАННЯ ФІШИНГОВИХ URL НА ОСНОВІ ЕВРИСТИЧНИХ ПРАВИЛ

Анотація. Зростаюча кількість кіберзагроз, зокрема фішингових атак, вимагає розробки ефективних методів виявлення фішингу. Фішинг є однією з найпоширеніших і найнебезпечніших форм кіберзлочинів, що спрямована на отримання доступу до конфіденційної інформації користувачів, маніпулюючи їх довірою. Методологія атак соціальної інженерії стрімко розвивається, що створює виклики для фахівців з кібербезпеки. У цьому дослідженні розглядається евристичний підхід на основі правил до виявлення фішингових URL-адрес, який для виявлення потенційних загроз аналізує різні характеристики вебадрес, такі як нетипова структура посилань, наявність підозрілих символів або неправильної послідовності слів у доменних іменах. Ментальна мапа, як інструмент візуалізації, забезпечує структурований і логічно впорядкований підхід до аналізу методів виявлення фішингових вебсайтів. Вона наочно демонструє взаємозв'язки між різними правилами, спрямованими на ідентифікацію підозрілої поведінки веб-ресурсів, а також дозволяє чітко простежити класифікацію характеристик, які притаманні фішинговим атакам. Дана мапа узагальнює ключові ознаки, що використовуються для аналізу URL-адрес, дозволяючи структуровано представити критерії оцінки потенційної загрози. Маючи наглядну класифікацію евристичних правил детектування, значно підвищується точність ідентифікації фішингових вебсайтів, захищаючи користувачів від можливих атак. У дослідженні оцінюється ефективність окремих евристичних правил та їх комбінацій, що дає уявлення про їхню застосовність до автоматизованих систем виявлення фішингу. Для цього використовуються ключові метрики, які визначають якість алгоритму та його здатність розрізняти фішингові та легітимні сайти, а саме достовірність, істинно позитивний рівень, рівень хибних спрацьовувань, точність, оцінка F-1. Результати демонструють доцільність евристичного виявлення як простої, ефективної та зрозумілої альтернативи складним моделям машинного навчання.

Ключові слова: фішинг; фішингові сайти; евристичні правила; класифікація; легітимна URL-адреса; ефективність правил.

ВСТУП

Розвиток цифрових технологій та глобальної мережі Інтернет відкрив безпрецедентні можливості для обміну інформацією, комунікації, ведення бізнесу, надання державних та фінансових послуг. Проте разом із зростанням обсягів онлайн-активності зростає і рівень загроз, пов'язаних із використанням інформаційних технологій у злочинних цілях [1]. Однією з найпоширеніших і водночас найнебезпечніших форм соціальної інженерії в кіберпросторі є фішинг — спроба

отримати конфіденційні дані користувачів шляхом обману, здебільшого через створення підроблених вебсайтів, які імітують легітимні ресурси [2].

Постановка проблеми. Зважаючи на масштабність і динамічність фішингових атак, а також їх здатність адаптуватися до нових умов, традиційні методи виявлення, що базуються лише на сигнатурному або чорному чи білому списках відомих доменів, часто виявляються недостатньо ефективними [3]. У відповідь на це зростає інтерес до методів, що дозволяють визначати шкідливу активність на основі поведінкових характеристик вебсайтів, зокрема через застосування евристичних правил, які враховують візуальні, структурні, мережеві та функціональні особливості фішингових ресурсів.

Стаття присвячена дослідженню методів виявлення фішингових вебсайтів на основі евристичних правил. Фішинг є однією з найпоширеніших і найнебезпечніших форм кіберзлочинів, що спрямована на отримання доступу до конфіденційної інформації користувачів, маніпулюючи їх довірою. Методологія атак соціальної інженерії стрімко розвивається, що створює виклики для фахівців з кібербезпеки.

Дослідження фокусується на евристичних підходах до аналізу веб-ресурсів, які дозволяють виявляти потенційно небезпечні вебсайти на основі структури URL-адреси, використання ненормальних функцій, підозрілих зовнішніх запитів та специфічної поведінки серверів.

Аналіз останніх досліджень і публікацій. При створенні класифікації методів детектування фішингових вебсайтів у даній роботі було проаналізовано низку наукових джерел, зокрема з акцентом на практичну застосовність та структурну логіку поділу. Основою для побудови узагальненої класифікації у вигляді ментальної мапи стало джерело Serhii Buchyk, Dmytro Shutenko and Serhii Toliupa «Phishing Attacks Detection». In: Information Technology and Implementation (IT&I-2022) [4], яке запропонувало чітке розділення методів на основі принципів їхньої роботи. Це дало змогу не лише систематизувати наявні підходи до виявлення фішингу, а й обрати найбільш доцільний напрямок подальшого дослідження. Дане джерело стало концептуальним орієнтиром при формуванні структурованої мапи методів, яка використовується в теоретичній частині роботи як основа для подальшого аналізу.

Мета статті. Систематизація, класифікація евристичних правил детектування фішингових сайтів на основі їхніх характеристик та розробка програмного забезпечення з метою покращення ефективності систем виявлення фішингу.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Фішинг — це спосіб соціальної інженерії, коли фальшиві повідомлення використовуються для крадіжки секретних даних або встановлення зловмисного софту [5]. Зловмисники маскуються під перевірені джерела, маніпулюючи емоціями, спонукаючи до термінових дій або обіцяючи призи. Згідно MITRE ATT&CK, у тактиці «Initial Access» техніка «Phishing» (T1566) включає чотири підтехніки: атаки через файли-вкладення, посилання, сторонні платформи та голосові зв’язки [6]. Фішингові вкладення та посилання поширюються через соціальні мережі та особисті поштові сервіси, використовуючи вкладення та посилання для обходу механізмів безпеки [7]. Поширеними ознаками фішингу є граматичні помилки, підозрілі посилання, запити на особисту інформацію та відчуття терміновості [8]. Для кращого виявлення фішингових сайтів можна застосовувати евристичні правила для аналізу URL-адрес.

ISSN 2663 - 4023

Методи евристичного аналізу дозволяють виявляти фішингові сайти на основі багатьох характеристик, таких як нетипова структура посилань, наявність підозрілих символів або неправильної послідовності слів у доменних іменах. Такі правила базуються на дослідженні шаблонів, які характеризують фішингові вебсайти, і дозволяють користувачам попереджати про потенційні загрози до того, як вони натиснуть посилання.

Для кращого розуміння правил їх можна класифікувати у декілька груп, а саме «Address Bar based Features», «HTML and JavaScript based features», «Domain based features», «Abnormal based features» [4].

Узагальнення евристичних правил, які були згруповані за окремими категоріями, дозволило створити класифікацію у вигляді ментальної мапи (рис.1), що є одним із ключових результатів даної роботи. Ментальна мапа, як інструмент візуалізації, забезпечує структурований і логічно впорядкований підхід до аналізу методів виявлення фішингових вебсайтів. Вона наочно демонструє взаємозв'язки між різними правилами, спрямованими на ідентифікацію підозрілої поведінки веб-ресурсів, а також дозволяє чітко простежити класифікацію характеристик, які притаманні фішинговим атакам. Дана мапа узагальнює ключові ознаки, що використовуються для аналізу URL-адрес, дозволяючи структуровано представити критерії оцінки потенційної загрози.

Рис. 1. Ментальна мапа класифікації евристичних правил детектування фішингових сайтів

Новизна запропонованого підходу полягає в інтеграції та вдосконаленні матеріалів, отриманих із різних джерел інформації, що дозволило систематизувати наявні методи детектування фішингу та подати їх у більш зручній для аналізу формі. Завдяки ментальній мапі спеціалісти з інформаційної безпеки отримують зручний інструмент для практичного використання у виявленні фішингових вебсайтів

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Реалізація моделі виявлення фішингових URL-адрес

У рамках даного дослідження було використано два набори даних, що містять URL-адреси: PhishingDataset.csv (рис. 2), який складається з фішингових посилань з сервісу PhishTank [9], та LegitimateDataset.csv (рис. 3), що містить легітимні URL-адреси. З обох датасетів були випадковим чином відібрані по 40000 посилань з більшого набору даних для забезпечення збалансованої вибірки і коректного аналізу.

Аналіз URL-адрес здійснювався за допомогою програми на мові програмування Python, яка реалізує низку евристичних правил для оцінки рівня довіри до вебресурсів. Зокрема, це дослідження базується на методології "функції на основі адресного рядка" (Address Bar based Features), що передбачає виявлення характерних ознак фішингових сайтів шляхом аналізу структури URL.

Програма зчитує набори даних, перевіряє кожне посилання на відповідність заданим правилам і підраховує, скільки з них відповідають певним критеріям. Для оцінки достовірності було використано вісім наборів функцій (рис.4), які поступово розширюють можливості перевірки даних. Спочатку застосовується перевірка на наявність у вебпосиланні IP-адреси в десятковому або шістнадцятковому вигляді. Надалі з кожною функцією додається по одному евристичному правилу: перевірка наявності «@», довжини URL-адреси, наявності перенаправлень, маркера «HTTPS/HTTP» у доменній частині, використання служб скорочення URL-адрес, наявності «-» та використання субдоменів.

То ж, аналіз полягав у визначенні того, скільки URL-адрес з кожного набору даних відповідають певним критеріям. Зібрані результати (рис. 5) дають змогу оцінити ефективність різних евристичних правил для автоматичного виявлення фішингових сайтів.

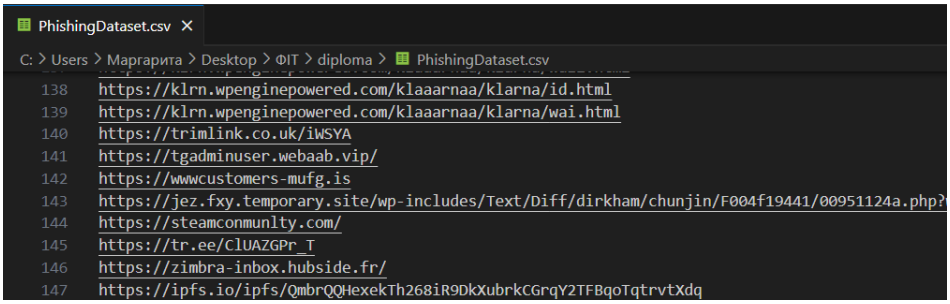

Рис. 2. Датасет фішингових URL-адрес

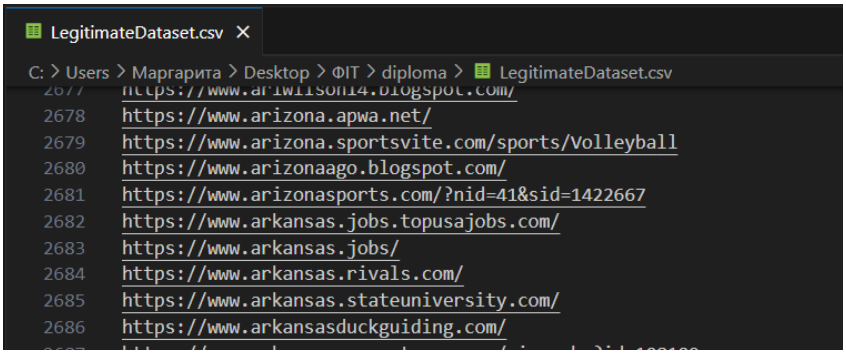

Рис. 3. Датасет легітимних URL-адрес

```
#Список наборів функцій для аналізу
function_sets = [
    [havingIP],
    [havingIP, haveAtSign],
    [havingIP, haveAtSign, getLength],
    [havingIP, haveAtSign, getLength, redirection],
    [havingIP, haveAtSign, getLength, redirection, httpDomain],
    [havingIP, haveAtSign, getLength, redirection, httpDomain, tinyURL],
    [havingIP, haveAtSign, getLength, redirection, httpDomain, tinyURL, prefixSuffix],
    [havingIP, haveAtSign, getLength, redirection, httpDomain, tinyURL, prefixSuffix, countSubdomains]
]
```

Рис. 4. Набори функцій для аналізу

```
PS C:\Users\Маргарита> & C:/Users/маргарита/AppData/Local/Programs/Python/Python312/python.exe
Function Set 1: Phishing = 340, Legitimate = 0
Function Set 2: Phishing = 830, Legitimate = 3
Function Set 3: Phishing = 17045, Legitimate = 1258
Function Set 4: Phishing = 17076, Legitimate = 1258
Function Set 5: Phishing = 17086, Legitimate = 1258
Function Set 6: Phishing = 18573, Legitimate = 4772
Function Set 7: Phishing = 25768, Legitimate = 6762
Function Set 8: Phishing = 31481, Legitimate = 7751
```

Рис. 5. Результат виконання програми

2. Аналіз ймовірностей спрацювання евристичних правил

Було проведено оцінку ймовірностей спрацювання кожного окремого правила, реалізованого як функції в розробленому програмному коді. Для кожного набору функцій було обчислено ймовірність спрацювання (табл. 1) та ймовірність їх появи (табл. 2) на фішингових ресурсах. Зібрані статистичні дані дали змогу проаналізувати кожне правило та визначити його внесок у загальну модель.

Таблиця 1

Ймовірності спрацювання евристичних правил

Правило	Ймовірність спрацювання
Використання IP-адреси	1
URL-адреса містить символ «@»	0,9916
Довга URL-адреса для приховування підозрілої частини	0,9776
Переспрямування за допомогою “//”	0,9686
Наявність маркера «HTTPS» у доменній частині URL-адреси	0,9685
Використання служб скорочення URL-адрес	0,8849
Додавання до домену префікса або суфікса, розділених «-»	0,8567
Субдомен і кілька субдоменів	0,8304

Отримані результати свідчать про високу ефективність використаних в програмному коді евристичних правил. Найбільш ймовірними ознаками фішингової поведінки стали використання IP-адрес замість доменних імен, наявність символу «@» в URL-адресі, надмірна довжина URL-адреси, використання механізму перенаправлення за допомогою подвійної косої риски та наявність «https» або «http» у доменній частині. Ці ознаки вказують на високий рівень виявлення, що підтверджується ймовірністю виявлення, близькою до 1. Менш поширені ознаки, такі як використання сервісів скорочення URL-адрес, наявність префіксів або суфіксів в доменних іменах і використання численних субдоменів, також є потенційно шкідливими ресурсами. Ці ознаки були зафіксовані з ймовірністю понад 0.8, що свідчить про їхню потенційну корисність у процесі виявлення загроз.

Для оцінки ефективності також має бути визначена ймовірність виявлення кожного правила на обраних з датасету URL-адресах. Ці ймовірності показують, наскільки часто певна ознака зустрічається серед них. Табл. 2 містить результати цього аналізу.

Таблиця 2

Розподіл виявлення евристичних правил

Правило	Ймовірність виявлення
Використання IP-адреси	0,0085
URL-адреса містить символ «@»	0,01225
Довга URL-адреса для приховування підозрілої частини	0,4054
Переспрямування за допомогою “//”	0,000775
Наявність маркера «HTTPS» у доменній частині URL-адреси	0,00025
Використання служб скорочення URL-адрес	0,0372
Додавання до домену префікса або суфікса, розділених «-»	0,1799
Субдомен і кілька субдоменів	0,1428

Табл. 2 демонструє розподіл ймовірностей виявлення різних евристичних правил. Аналіз показує, що деякі ознаки зустрічаються значно частіше, наприклад, маніпуляції з довжиною URL-адреси, використання субдоменів або додавання префіксів і суфіксів до доменного імені. Інші характеристики, зустрічаються рідше, але все ще можуть свідчити про потенційну загрозу.

Загалом, отримані дані підтверджують ефективність застосування комплексу евристичних правил для виявлення фішингових сайтів, оскільки навіть малопоширені ознаки в сукупності допомагають ідентифікувати шкідливі ресурси. В сумі ймовірності всіх правил дорівнюють 0.787, що і є істинно позитивним рівнем спрацювання усіх правил в сукупності.

3. Ефективність спрацювання правил

Після попереднього етапу аналізу, який базується на спрацюванні евристичних правил класифікації ознак на основі адресного рядка для виявлення фішингових сайтів, необхідно оцінити ефективність розробленої моделі. Для цього використовуються ключові метрики, які визначають якість алгоритму та його здатність розрізняти фішингові та легітимні сайти, а саме достовірність, істинно позитивний рівень, рівень хибних спрацьовувань, точність, оцінка F-1 [10].

Достовірність (Accuracy) показує, наскільки правильно класифіковані раніше евристичні правила визначили усі перевірені URL-адреси

$$Accuracy = \frac{31481 + 32249}{31481 + 32249 + 7751 + 8519} = 0{,}7966. \quad (1)$$

Істинно позитивний рівень (TPR), також відомий як Recall, дозволяє оцінити, якою мірою метод виявляє фішингові сайти, не залишаючи їх без уваги. Високий TPR означає, що алгоритм ефективно виявляє фішингові загрози; низький TPR означає, що багато фішингових сайтів залишаються нерозпізнаними, що є серйозною проблемою для безпеки користувачів.

$$TruePositiveRate(Recall) = \frac{31481}{31481 + 8519} = 0{,}787. \quad (2)$$

Рівень хибних спрацьовувань відображає частку легітимних сайтів, помилково класифікованих як фішингові. Якщо FPR алгоритму занадто високий, це означає, що його прогнози надто агресивні і можуть негативно вплинути на користувачів, оскільки

вони можуть втратити доступ до легальних ресурсів. У таких випадках необхідно оптимізувати евристичні правила, щоб знизити FPR без суттєвого зменшення TPR.

$$FalsePositiveRank = \frac{7751}{7751 + 32249} = 0{,}1938. \quad (3)$$

Точність показує, яка частка всіх вебсайтів, які алгоритм ідентифікує як фішингові, насправді є фішинговими. Висока точність означає, що алгоритм рідко помиляється у виявленні загроз і має мало хибних спрацьовувань.

$$Precision = \frac{31481}{31481 + 7751} = 0{,}8024. \quad (4)$$

Так як оцінка F-1 є середнім гармонійним значенням точності і істинно позитивним рівнем, а отже, дозволяє оцінити, наскільки добре алгоритм балансує між виявленням загроз і мінімізацією хибних спрацьовувань. Ця метрика особливо корисна, коли важливо уникнути помилкової класифікації легальних сайтів, а також виявлення фішингових сайтів; високе значення F1 означає, що алгоритм успішно вирішує обидва завдання – правильного виявлення загроз і мінімізації помилкових спрацьовувань.

$$F1 - Score = 2 \times \frac{0{,}8024 \times 0{,}787}{0{,}8024 + 0{,}787} = 0{,}7946. \quad (5)$$

Отримане значення F1-score = 0.7946 свідчить про достатньо високий рівень ефективності застосованих евристичних правил. Це означає, що алгоритм демонструє хорошу збалансованість між точністю та повнотою, що особливо важливо для задач кібербезпеки, де як помилкове блокування легітимних сайтів (False Positives), так і пропуск фішингових загроз (False Negatives) можуть мати серйозні наслідки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Класифікація евристичних правил у вигляді ментальної мапи дозволяє ідентифікувати специфічні патерни активності, які є типовими для фішингових ресурсів, наприклад, неправильна інтеграція зовнішніх джерел чи маніпулятивна обробка введених користувачами даних. Маючи наглядну класифікацію евристичних правил детектування, значно підвищується точність ідентифікації фішингових вебсайтів, захищаючи користувачів від можливих атак. Ця точність вимірюється за допомогою ключових метрик ефективності алгоритму.

Продуктивність розробленої системи виявлення була кількісно оцінена за допомогою ключових показників класифікації, таких як точність, повнота, F1-оцінка та коефіцієнт хибнопозитивних результатів. Досягнутий F1-бал, що дорівнює 0.7946, демонструє досить високу ефективність евристичного підходу лише згідно однієї групи правил з класифікації. Результати дослідження підтвердили, що комплексний підхід до виявлення фішингових сайтів є найефективнішим.

Проведена робота не лише систематизує знання про сучасні методи виявлення фішингових сайтів, але й забезпечує практичну основу для створення автоматизованих систем захисту від однієї з найнебезпечніших форм соціальної інженерії — фішингу. Впровадження таких систем дозволяє мінімізувати ризики компрометації даних, підвищуючи рівень безпеки як для окремих користувачів, так і для організацій, що особливо актуально в умовах постійного ускладнення методів зловмисників та їх адаптації до нових технологій.

Поєднуючи класичні евристичні правила з систематичним аналізом, дослідження закладає основу для адаптивних систем захисту, які можна інтегрувати в існуючі інфраструктури кібербезпеки. Враховуючи еволюціонуючий характер тактики фішингу, майбутні дослідження повинні зосередитися на впровадженні машинного навчання та методів штучного інтелекту для підвищення гнучкості та стійкості системи до нових загроз. Впровадження таких систем дозволяє мінімізувати ризики компрометації даних, підвищуючи рівень безпеки як для окремих користувачів, так і для організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mashtalir, V. et al. (2024). Kiberborot'ba v umovakh zbroinoho protystoiannia: analiz, stratehii ta vyklyky. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 49(1),* 93–104. https://doi.org/10.33099/2311-7249/2024-49-1-93-104
2. Alkhalil, Z. та ін. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3.* https://doi.org/10.3389/fcomp.2021.563060
3. Marchal, S., Saari, K., Singh, N., & Asokan, N. (2016). Know your phish: Novel techniques for detecting phishing sites and their targets. *In Proceedings of the IEEE 36th International Conference on Distributed Computing Systems (ICDCS),* 323–333. https://doi.org/10.48550/arXiv.1510.06501
4. Buchyk, S., Shutenko, D., & Toliupa, S. (2022). Phishing Attacks Detection. *In IX International Scientific Conference "Information Technology and Implementation" (IT&I-2022), Workshop Proceedings,* 193–201. https://ceur-ws.org/Vol-3384/Short_7.pdf
5. *What is phishing? | Microsoft security suite.* (n.d.). Microsoft. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing
6. *Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*. (n.d.). MITRE ATT&CK®. https://attack.mitre.org/techniques/T1566/
7. Alabdan, R. (2020). Phishing attacks survey: types, vectors, and technical approaches. *Future Internet, 12(10),* 168. https://doi.org/10.3390/fi12100168
8. Mohammad, R., Thabtah, F., & Mccluskey, T. (2012). An assessment of features related to phishing websites using an automated technique. *In 2012 International Conference on Information and Computer Science (ICICS),* 492–497. https://ieeexplore.ieee.org/document/6470857
9. *Phishtank*. (n.d.). https://www.phishtank.com
10. Ozcan, A., et al. (2021). A hybrid DNN–LSTM model for detecting phishing URLs. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-021-06401-z

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Serhii Buchyk
DSc (Engin.), Prof.,
Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0003-0892-3494
buchyk@knu.ua

Marharyta Tolstiak
Student of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0009-0007-9221-8187
tolstiakm@knu.ua

DETECTING PHISHING URLS BASED ON HEURISTIC RULES

Abstract. The growing number of cyber threats, including phishing attacks, requires the development of effective phishing detection methods. Phishing is one of the most widespread and dangerous forms of cybercrime aimed at gaining access to confidential user information by manipulating their trust. The methodology of social engineering attacks is evolving rapidly, which creates challenges for cybersecurity professionals. This study discusses a rule-based heuristic approach to detecting phishing URLs that analyses various characteristics of web addresses, such as atypical link structure, suspicious characters, or incorrect word sequences in domain names, to identify potential threats. A mind map, as a visualisation tool, provides a structured and logically ordered approach to analysing phishing website detection methods. It clearly demonstrates the relationships between various rules aimed at identifying suspicious behaviour of web resources, and also allows you to clearly trace the classification of characteristics inherent in phishing attacks. This map summarises the key features used to analyse URLs, allowing for a structured presentation of the criteria for assessing a potential threat. Having a clear classification of heuristic detection rules, the accuracy of identifying phishing websites is significantly improved, protecting users from possible attacks. The study evaluates the effectiveness of individual heuristic rules and their combinations, which gives an idea of their applicability to automated phishing detection systems. For this purpose, we use key metrics that determine the quality of the algorithm and its ability to distinguish between phishing and legitimate websites, namely reliability, true positive rate, false positive rate, accuracy, and F-1 score. The results demonstrate the feasibility of heuristic detection as a simple, effective and understandable alternative to complex machine learning models.

Keywords: phishing; phishing sites; heuristic rules; classification; legitimate URL; rule effectiveness.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Mashtalir, V. et al. (2024). Kiberborot'ba v umovakh zbroinoho protystoiannia: analiz, stratehii ta vyklyky. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 49(1),* 93–104. https://doi.org/10.33099/2311-7249/2024-49-1-93-104
2. Alkhalil, Z. та ін. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3.* https://doi.org/10.3389/fcomp.2021.563060
3. Marchal, S., Saari, K., Singh, N., & Asokan, N. (2016). Know your phish: Novel techniques for detecting phishing sites and their targets. *In Proceedings of the IEEE 36th International Conference on Distributed Computing Systems (ICDCS),* 323–333. https://doi.org/10.48550/arXiv.1510.06501
4. Buchyk, S., Shutenko, D., & Toliupa, S. (2022). Phishing Attacks Detection. *In IX International Scientific Conference "Information Technology and Implementation" (IT&I-2022), Workshop Proceedings*, 193–201. https://ceur-ws.org/Vol-3384/Short_7.pdf
5. *What is phishing? | Microsoft security suite.* (n.d.). Microsoft. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing
6. *Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*. (n.d.). MITRE ATT&CK®. https://attack.mitre.org/techniques/T1566/

7. Alabdan, R. (2020). Phishing attacks survey: types, vectors, and technical approaches. *Future Internet, 12(10),* 168. https://doi.org/10.3390/fi12100168
8. Mohammad, R., Thabtah, F., & Mccluskey, T. (2012). An assessment of features related to phishing websites using an automated technique. *In 2012 International Conference on Information and Computer Science (ICICS),* 492–497. https://ieeexplore.ieee.org/document/6470857
9. *Phishtank*. (n.d.). https://www.phishtank.com
10. Ozcan, A., et al. (2021). A hybrid DNN–LSTM model for detecting phishing URLs. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-021-06401-z