КОМПЛЕКС ЩОДО ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Кожушко Д.Р.
Науковий керівник – к.т.н., доц. Федюшин О.І.
Харківський національний університет радіоелектроніки
(61666, м. Харків, пр. Науки 14, каф. Безпеки інформаційних технологій,
тел. (057) 702-14-25, email: d_its@nure.ua)

The given work is dedicated to the best practices of awareness of phishing attacks. Phishing attacks are usually very massive, so they can touch anybody. Basic behavior rules can help people save from most attacks and protect their personal data.

Фішинг (англ phishing від fishing – риболовля) – це злочинне діяння в Інтернеті, яке відбувається, коли зловмисна веб-сторінка видає себе за законну веб-сторінку з метою отримання конфіденційної інформації від користувача [1].

Ці методи зазвичай включають шахрайську електронну пошту та веб-сайти, які видають себе за законні електронну пошту та веб-сайти. Шахрайські електронні листи можна вважати зловмисною формою небажаної масової електронної пошти, загальновідомої як "спам". Звичайні користувачі вразливі до крадіжки особистих даних та деяких фінансових втрат через шахрайські операції. Фінансові установи ризикують через велику кількість шахрайських операцій із використанням викраденої інформації.

Фішинг-атаки часто є дуже масштабними подіями, які спрямовані на тисячі споживачів або більше, в надії, що на певний відсоток захоче відповісти. Відносно великий відсоток одержувачів відповідають на електронні листи, оскільки вони видаються законними, і їх автентичність неможливо легко перевірити. Оцінки рівня відповіді коливаються від 1% до 20%, залежно від атаки [2].

Оскільки між зловмисником та споживачем не існує особистого контакту, споживач має дуже мало інформації для роботи, щоб вирішити, чи є електронний лист або веб-сайт законним.

Метою даного дослідження є вирішення проблеми ефективної фільтрації веб-сайтів на предмет виявлення потенційно фішингового контенту за рахунок розробки та використання спеціалізованого програмного додатку для боротьби зі злочинним контентом.

На сьогодні найбільше розповсюдження для захисту від фішингу отримали наступні методи: 1) використання настільних програм антиспам-фільтрації; 2) використання служб конфіденційності комп’ютера; 3) введення веб-адреси та перевірка її на справжність; 4) встановлення антивірусного та антишпигунського програмного забезпечення.

Перелічені методи мають свої переваги та недоліки. Більшість підходів зводиться до використання спеціалізованого, як правило, комерційного

програмного забезпечення з метою блокування можливостей шахраїв. Подібне програмне забезпечення вимагає тонкого налаштування засобів фільтрації та довіри до технічної реалізації аналізу, адже постачальники досить рідко розкривають використовувані технології аналізу, а також надають інформацію про кількість хибних спрацьовувань. Більшість з них мають складний інтерфейс налаштування, встановлюються як окремі плагіни та додатки на машину клієнта, рідко оновлюються.

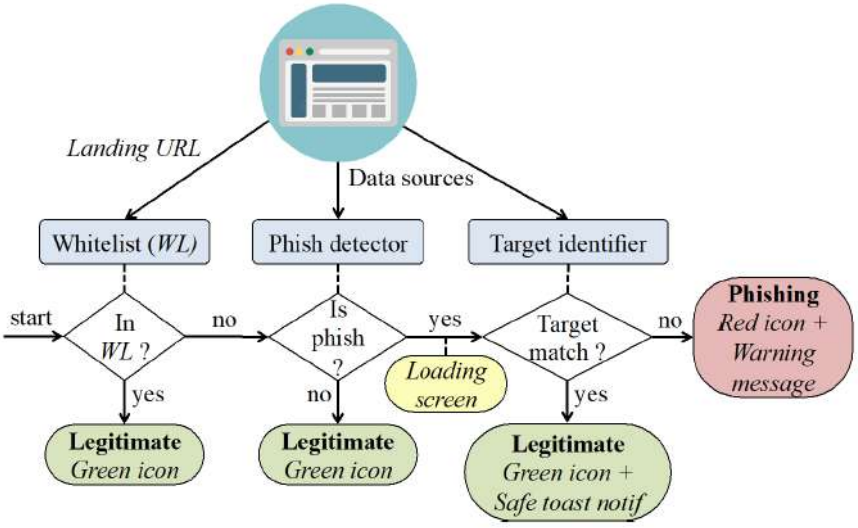

Рисунок 1 – Алгоритм аналізу на предмет фішингу

Запропонований в роботі програмний додаток використовує в своїй архітектурі алгоритм аналізу контенту сайтів по трьох основних складових (див. рис. 1): перевірка за технологією білих списків, детектора фішингового контенту та аналізу потенційного URL для переходу.

Цей підхід дозволяє автоматично виявляти та видаляти шкідливе програмне забезпечення та блокувати вихідну доставку конфіденційної інформації зловмисним сторонам. В своїй роботі комплекс не використовує комерційної складової тобто може бути вільно розповсюдженим.

Список використаної літератури:

1. Jeeva, S.C., Rajsingh, E.B. Intelligent phishing url detection using association rule mining.//Hum. Cent. Comput. Inf. Sci. 6, 10 (2016). https://doi.org/10.1186/s13673-016-0064-3.

2. Tally, G., R. Thomas and Tom Van Vleck. Anti-Phishing: Best Practices for Institutions and Consumers. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: https: //www.semanticscholar.org/paper /Anti-Phishing%3A-Best-Practices-for-Institutions-and-Tally Thomas/3e5ae0fb6cba 7c975bb2ca2da50b659e98493441.