Статья 1: МОДЕЛЬ ОБНАРУЖЕНИЯ ФИШИНГОВЫХ АТАК НА ОСНОВЕ ГИБРИДНОГО ПОДХОДА ДЛЯ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

В статье описывается архитектура системы обнаружения фишинговых атак.

Используемые эвристики:

Производится проверка кода страны домена и кода страны хостинг-провайдера;

URL проверяется на фишинговые ключевые слова;

Производится проверка валидности SSL/TSL – сертификата;

Проверка длины URL, если длина более 60 символов, сайт считается подозрительным;

При обнаружении в URL символа “@”, сайт считается подозрительным;

Проверка URL на количество точек;

Проверка наличия двух слешей после протокольной части, более одной протокольной части и более одного порта в URL-адресе;

Оценка доступности URL.

Статья 2: ИСПОЛЬЗОВАНИЕ МОДЕЛИ НЕЧЕТКИХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ФОРМИРОВАНИЯ БАЗЫ ЗНАНИЙ ПО ОПРЕДЕЛЕНИЮ ФИШИНГОВЫХ САЙТОВ

В статье приходят к выводу, что создание системы обнаружения вредоносных URL-адресов в реальном времени является лучшим способом для борьбы с фишингом. Была построена модель нечетких нейронных сетей. Для анализа было собрано 50 тысяч URL адресов. Было использовано 6 параметров: длина URL, длина домена, наличие тире в доменном имени, наличие символа @, является ли URL-адрес ip-адресом, количество поддоменов.

Точность определения фишинговых сайтов, с использованием различных методов машинного обучения составила от 90% до 95,9%. Наиболее высокая точность достигалась с использованием классификатора на основе коллектива нечетких нейронных сетей.

Статья 3: БОРЬБА С ФИШИНГОМ ПРИ ПОМОЩИ CLAMAV

ClamAV – программный продукт для определения фишинг адресов.

ClamAV поддерживает два метода определения фишинг-адресов: эвристический и на основании сигнатур.

В ClamAV используется две базы: main и daily. Первая – постоянная, вторая – для ежедневных обновлений.

Порядок проверки на фишинг:

- проверяется совпадение RealURL=DisplayedURL, если совпадает, то проверка заканчивается;

- нормализация URL (убираются лишние символы, символы «\» заменяются на «/», адрес приводится к верхнему регистру и так далее);
- проверяется адрес в WDB (белая БД), при обнаружении проверка заканчивается;
- извлекается домен и имя узла, которые также сверяются с WDB;
- проверяется наличие закодированного IP-адреса;
- проверяется наличие SSL в RealURL (если DisplayedURL использует http, а в RealURL – https, то заблокировать такие ссылки можно, установив PhishingAlwaysBlockSSL Mismatch в yes);
- если на месте RealURL вместо имени стоит IP-адрес, такой узел блокируется;
- далее проверяется соответствие в RealURL и DisplayedURL сначала имени узла, а затем домена, при совпадении проверка заканчивается.

Статья 4: СИСТЕМА ПРОТИВОДЕЙСТВИЯ ФИШИНГ АТАКАМ

Предлагается модель для предотвращения фишинговых атак, результатом которой является блокировка попыток пользователя загрузить фишинговый сайт. Схема модели представлена на рисунке 3.

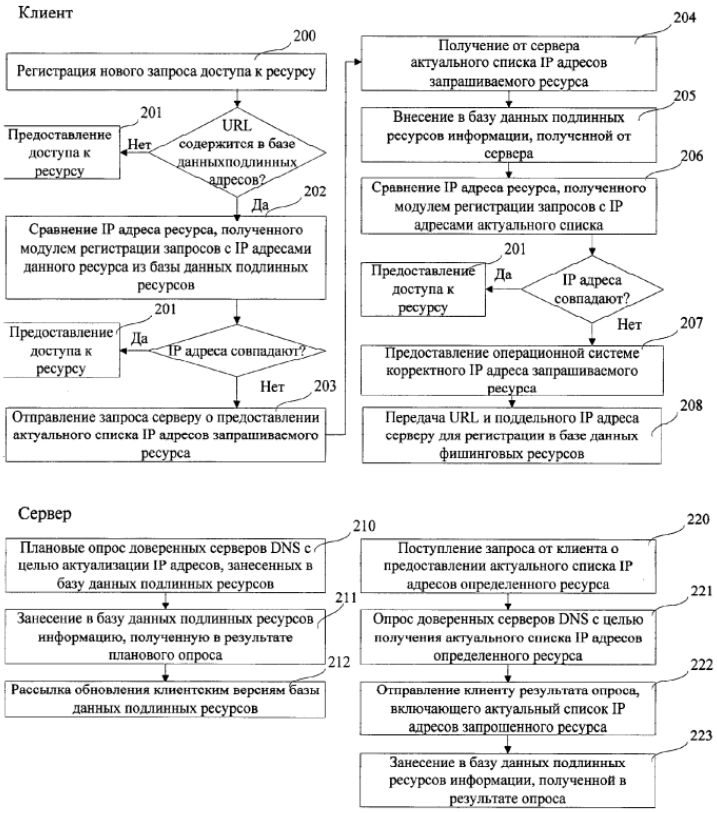

Рисунок 1 - Блок-схема модели

Статья 5: СИСТЕМА И СПОСОБ ФОРМИРОВАНИЯ ПРАВИЛ ПОИСКА ДАННЫХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ФИШИНГА

В статье предлагается система правил поиска данных, исходя из которых будут определяться фишинговые ресурсы.

Одним из способов построения правил является использование нейронной сети, которая может обучаться формированию новых более точных правил на основе параметров, полученных при обработке полученных ранее данных.

Структура системы: средство перехвата, передаваемых от сервера клиенту и передачи данных средству категоризации, средство категоризации, предназначенное для определения, по меньшей мере, одной категории перехваченных данных, и передачи данных, разделенных на категории, средству анализа данных, средство анализа данных, предназначенное для поиска по данным, разделенным на категории, признаков фишинга, вычисления параметров признаков фишинга и передачи их средству формирования правил, средство формирования правил, предназначенное для формирования по вычисленным параметрам признаков фишинга.

Статья 6: СИСТЕМА И СПОСОБ СБОРА ИНФОРМАЦИИ ДЛЯ ОБНАРУЖЕНИЯ ФИШИНГА

Предлагается способ для обнаружения фишинговых ресурсов при помощи сбора URL ссылок, включающий следующие шаги:

- получение на веб-сервере, на котором располагается веб-ресурс, запроса по протоколу http/https на получение ресурса, расположенного на данном веб-ресурсе;

- извлечение из поля referrer запроса URL-ссылки, указывающей на источник запроса;

- генерирование на основании извлеченной URL-ссылки по крайней мере одной преобразованной URL-ссылки, ссылающейся на другой ресурс, расположенный на том же хосте. В итоге, чтобы произвести переход на корневую директорию

- передача на анализ наличия фишинга по крайней мере одной преобразованной ссылки

Статья 7: АНАЛИЗ ТЕХНИК РЕАЛИЗАЦИИ ФИШИНГАТАК

В html-коде для большей убедительности используют ссылки на легитимные ресурсы. Как правило, это FAVorites ICON – значки веб-ресурсов.

Вставка символа «@», так жертва будет попадать на ресурс, указанный после этого символа, а не перед ним.

Применение IDN. Некоторые буквы в разных алфавитах имеют схожее написание.

Помимо ссылок, приводящих пользователя на фишинговый веб-ресурс, злоумышленники прикрепляют к сообщениям вредоносное вложение или ссылку, при нажатии которых начинается загрузка программного обеспечения и незаметное встраивание в систему жертвы. Чаще всего вредоносный скрипт находится внутри документа с популярным расширением. Это такие форматы, как .zip, .xls, .pdf. Атака в большинстве случаев проходит успешно, так как у жертвы по умолчанию активирована настройка «скрывать расширение для зарегистрированных типов файла».

Вредоносное вложение можно спрятать в картинке. Злоумышленники используют векторные изображения, так как их не обнаруживают средства защиты, в отличии от растровых.

Статья 8: ИССЛЕДОВАНИЕ ТЕХНИК ФИШИНГА И МЕТОДОВ ЗАЩИТЫ ОТ НЕГО

Существуют системы противодействию фишингу, в которых используется подход сравнения запрошенных адресов сайтов с черным списком адресов, либо с белым списком, такие системы сталкиваются с проблемами: устаревшие базы данных, в случае с черным списком адресов и подмена IP адреса запрашиваемого ресурса, при прежнем названии и домене в составе URL.

Можно применять машинное обучение, где по совокупности различных характеристик сайта определяется уровень доверия к нему. Рассматриваются как внешний вид сайта, так и его регистрационные данные.

Статья 9: ВИДЫ ФИШИНГА И СПОСОБЫ ЗАЩИТЫ ОТ НЕГО

Приводится в пример вид фишинга, когда на первом этапе на ПК внедряется ПО, активирующееся в момент, когда пользователь посещает необходимый web-сайт, далее происходит процесс подмены. Вместо проверенного сайта пользователь попадает на фишинговый. Подмена осуществляется путем изменения кэша DNS на локальном компьютере или сетевом оборудовании.

Статья 10: РАЗРАБОТКА ПРОГРАММНО-МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОАНАЛИТИЧЕСКОГО МОНИТОРИНГА ФИШИНГОВЫХ АТАК

Проверка доменных имен схожих по написанию с подлинными интернет-ресурсами, может производиться с использованием алгоритма основанного на расстоянии Левенштейна, которое определяет с через разность последовательности их символов. С помощью расстояния Левенштейна можно обнаружить замену одного символа на другой, его отсутствие или добавление лишнего.

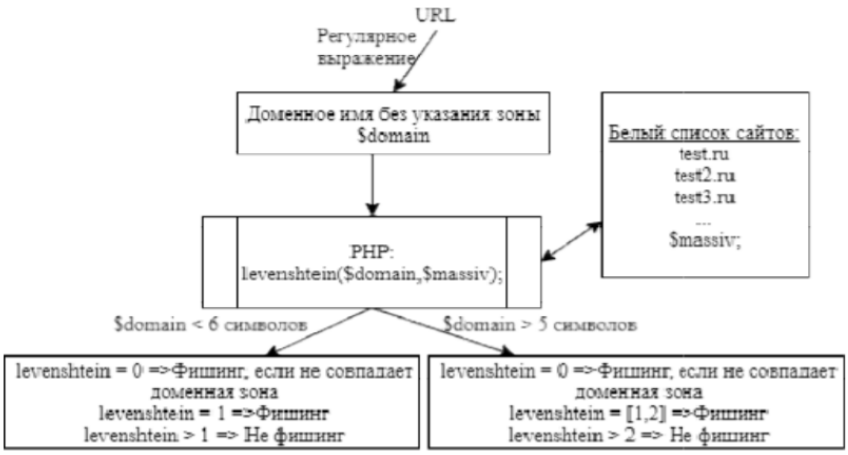

Рисунок 2 – Алгоритм выявления фишинга через расстояние Левенштейна

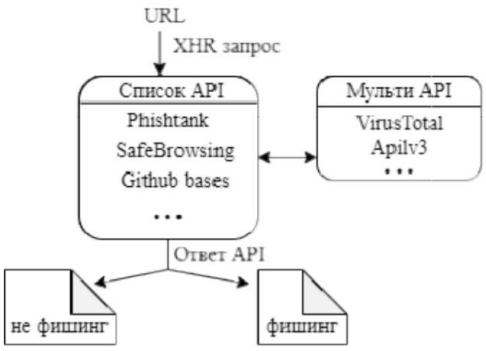

Рисунок 3 - Алгоритм выявления фишинга через черные списки сайтов