

СИСТЕМА ЗАЩИТЫ ОТ
ФИШИНГА И СПАМА






KAIROS

AVSOFT




ПРОБЛЕМА

Фишинг и спам наиболее простые и востребованные способы проникновения в организацию вирусом




Источники

-  Документы
-  Мессенджеры
-  Социальные сети
-  Электронная почта
-  Магазин приложений

Виды жертв

-  Большие группы пользователей
-  Конкретные пользователи
-  Топ-менеджеры и руководители

Цели

-  Рассылка вирусов
-  Получение личных данных
-  Промышленный шпионаж

KAIROS

Система защиты от фишинга и спама KAIROS специализированное решение для анализа веб-ссылок и содержимого сообщений на предмет нелегитимности и необходимости пользователю

Технологии



DKIM, DMARC и SPF



Динамический анализ



Антивирусная проверка



Статический анализ



Модели машинного обучения



Внешние аналитические сервисы и базы данных

ТЕХНОЛОГИЯ РАБОТЫ



* Система KAIROS может выступать самостоятельным почтовым шлюзом и выполнять доставку писем получателям

АНАЛИТИЧЕСКИЙ ПОТЕНЦИАЛ

Анализируя при помощи ML структурные особенности URL-адреса и содержимое страницы фишингового веб-сайта, извлекается 17 категорий признаков (более 800 признаков)



Статистические признаки



Анализ ключевых слов в адресе и странице



Внешние сервисы (алекса, whois, pagerank и др)



Анализ dns, сертификата ssl и владельца и др



Содержимое страницы (анализ кода страницы и js)



Динамика переходов по ссылке

Виды моделей

RandomForest
(PHISHING.dill)

Нейронная сеть
(neuro_PHISHING.h5)

Catboost
(model_Cat_*)

АНАЛИЗ ВЕБ-ССЫЛОК

Проверка веб-ссылок осуществляется одновременно в нескольких направлениях



Модели ML



Проверка редиректов



Статический анализ



Внешние сервисы

XSEO

Phish Tank

Urlscan

VirusTotal Domain

VirusTotal URL

ПРОВЕРКА ФИШИНГА

Компрометация

НН (приглашение на собеседование) или LinkedIn

Знакомства

Банк (письмо от банка или руководителя с просьбой оплатить)

COVID-19

Клон (клонирование легитимного письма с подменой)

Подписки

Катастрофа или просьба срочной помощи

Игры

МАШИННОЕ ОБУЧЕНИЕ

В системе KAIROS присутствует ансамбль моделей, что дает более высокую надежность и точность вынесения вердикта.



ТРАНСФОРМЕРЫ

Использование для классификации и обработки текстов трансформеров, хорошо понимают контекст предложения, его настроение и общий смысл



ИЗВЛЕЧЕНИЕ ПРИЗНАКОВ

Для получения вектора признаков используется концепция вложений (embeddings), который способен определять связи между словами, их многозначность, последовательность, преобразование, контекст, частоту



МУЛЬТИЯЗЫЧНОСТЬ

Поддержка 15 языков: арабский, китайский, голландский, английский, французский, немецкий, итальянский, корейский, польский, португальский, русский, испанский, турецкий



ДООБУЧЕНИЕ

Предусмотрена возможность автоматического и ручного (самостоятельно пользователем) дообучение моделей, с возможностью выбора категории по темам



ЗАЩИТА И СКОРОСТЬ

Для защиты моделей от отравления и компрометации в системе предусмотрен контрольный датасет, по которому отслеживаю метрики дообученных моделей.



БОТЫ

Боты в сети Интернет собирают для моделей данные в автоматическом режиме, которые при достижении критической массы используются для дообучения моделей и повышения их эффективности

ПОЛИТИКИ

Система KAIROS имеет
гибкую систему политик
и правил фильтрации

Настройка правил
проверки по
IP адресу источника



Блокировка почтового
адреса при превышении
лимитов по спаму



Сессии почтового
сервера



Репутация
источника



Постобработка писем
для ретроспективного
анализа



Рейтинг получателя

ОСОБЕННОСТИ

Система ботов актуализирует базу данных по IP-адресам, доменам, веб-ссылкам и визуальному контенту сайтов



Модели машинного обучения могут осуществлять процесс своего дообучения самостоятельно в автоматическом режиме



Система может быть интегрирована с любыми сервисами и подключить к себе необходимые дополнительные источники

БЕЗОПАСНОСТЬ СИСТЕМЫ



ИНТЕГРАЦИЯ И РАЗВЕРТЫВАНИЕ

Система KAIROS может быть интегрирована по API интерфейсу



Межсетевой экран



Антивирусный мультисканер



Антиспам система



Песочница



DLP



Система KAIROS поддерживает несколько сценариев развёртывания



Физическая инфраструктура



Виртуальная инфраструктура



Облачная инфраструктура

РЕЖИМ РАБОТЫ

Протоколы проверки

• SMTP

• POP3

• IMAP

Зеркалирование

Приём вcc копии трафика для анализа, результаты проверки письма пользователем отображаются постфактум



Гибридный режим

Возможность указания определенных серверов для проверки в качестве полноценного почтового шлюза, а от других принимать на проверку в режиме зеркалирования



Почтовый шлюз

Система выступает в качестве MTA и для настройки требуется изменение DNS MX записи для перенаправления трафика, далее результаты проверки система передаёт почтовому серверу заказчика



КОНТАКТЫ

Спасибо, что нашли
время ознакомиться
с презентацией!



+7 (495) 988-92-25



office@avsw.ru



127106, г. Москва,
ул. Гостиничная, д.5



www.avsw.ru