

СИСТЕМА ЗАЩИТЫ ОТ
СПАМА И ФИШИНГА

KAIROС

AVSOFT

ПРОБЛЕМА

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

Электронная почта является наиболее простым способом проникновения вирусов.

По данным аналитического агентства CSO Online 94% всех вредоносных программ доставляется по электронной почте.

Виды жертв

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

Цели

-  Рассылка вирусов
-  Получение личных данных
-  Промышленный шпионаж

KAIROС

Система защиты от спама и фишинга на базе анализа текстовых сообщений, веб-ссылок и вложений в электронных письмах и других каналах передачи данных

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



Анализ ключевых слов в адресе и странице



Проверка трех стандартов безопасности: SPF, DKIM, DMARK



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_*)

Трансформеры

ПРОВЕРКА ФИШИНГА

Типы



Массовый



Адресный

Виды



Текстовый



Голосовой



Видео-композиции

Маски

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

АНАЛИЗ ВЕБ-ССЫЛОК

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



Модели ML



Проверка редиректов



Статический анализ



Внешние сервисы

XSEO

Phish Tank

Urlscan

VirusTotal Domain

VirusTotal URL

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



ЗАЩИТА И СКОРОСТЬ

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

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

Предусмотрена возможность автоматического и ручного дообучения моделей, с возможностью выбора категории по темам



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



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

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

БЕЗОПАСНОСТЬ СИСТЕМЫ



РЕЖИМ РАБОТЫ

Протоколы проверки

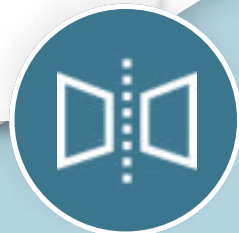
• SMTP

• POP3

• IMAP

Зеркалирование

Приём всех 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 МТА 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