

ПРОБЛЕМА

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

Источники





Социальные сети

Электронная почта

Магазин приложений



Виды жертв

у Большие группы пользователей

Конкретные пользователи

Топ-менеджеры и руководители

Цели

Рассылка вирусов

б Получение личных данных

Промышленный шпионаж



РЕШЕНИЕ

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

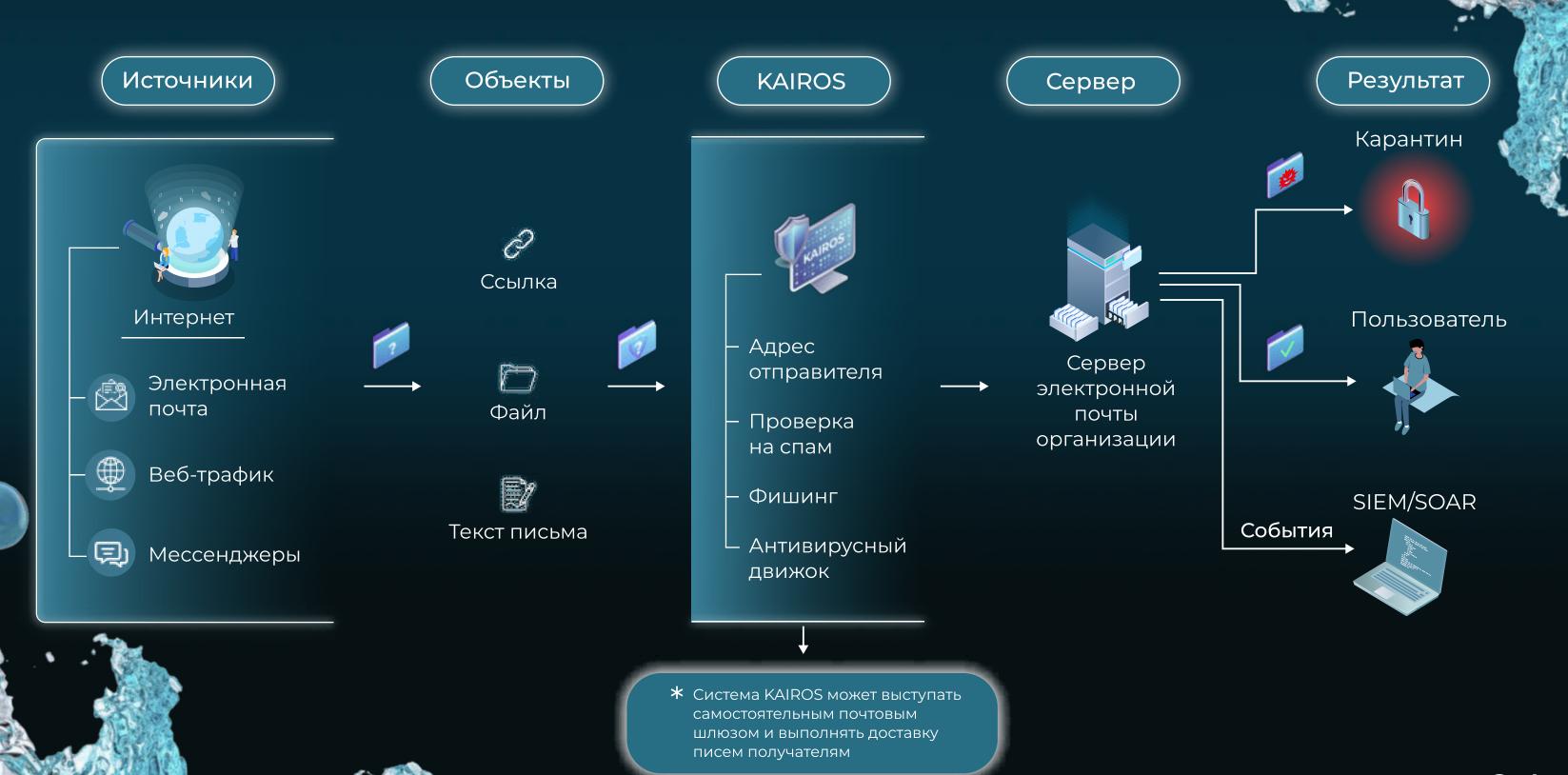


Модели машинного обучения



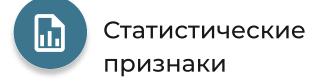
Внешние аналитические сервисы и базы данных

ТЕХНОЛОГИЯ РАБОТЫ



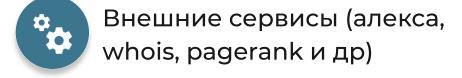
АНАЛИТИЧЕСКИЙ ПОТЕНЦИАЛ

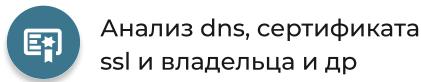
Анализируя при помощи ML структурные особенности URL-адреса и содержимое страницы фишингового веб-сайта, извлекается 17 категорий признаков (более 800 признаков)

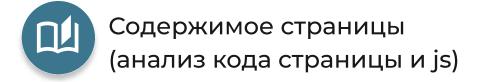




Анализ ключевых слов в адресе и странице

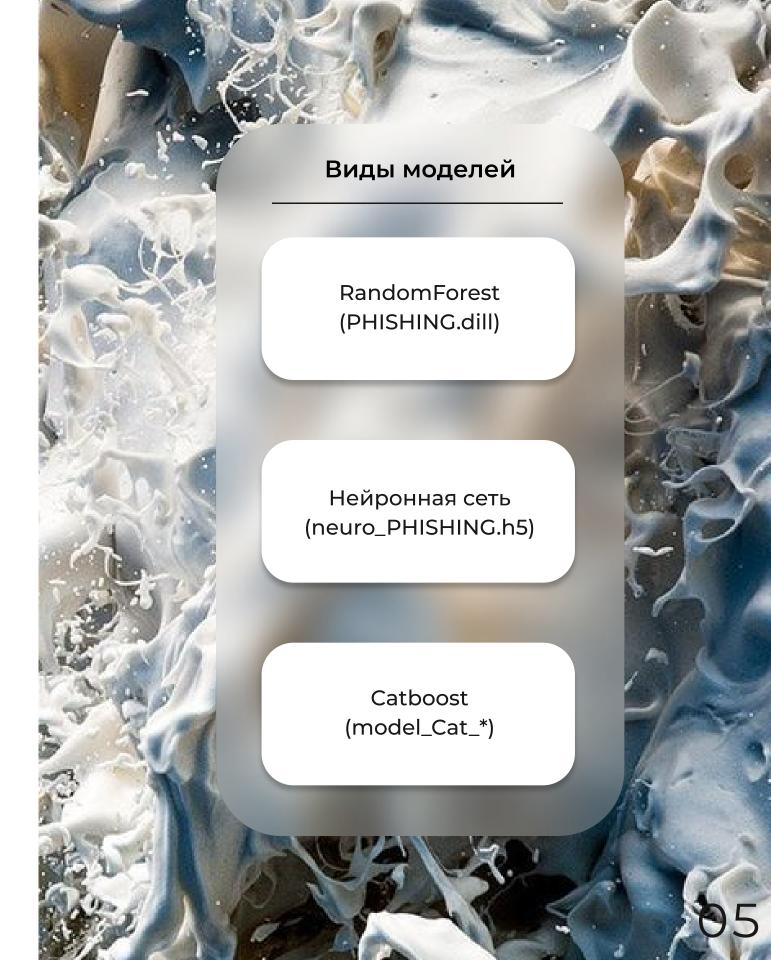








Динамика переходов по ссылке





АНАЛИЗ ВЕБ-ССЫЛОК

Проверка веб-ссылок осуществляется одновременно в нескольких направлениях







ПРОВЕРКА ФИШИНГА



Компрометация

HH (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 системы 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





БЕЗОПАСНОСТЬ СИСТЕМЫ

Мониторинг и обновление инфраструктурных модулей системы



Ролевая модель с тонкой настройкой доступа к функционалу



Блокировка неактивных учетных записей и периодическая принудительная смена пароля



Система KAIROS имеет политики и настройки для обеспечения собственной безопасности



Регистрация авторизации в системе пользователей и посредством АРІ интерфейса



Фиксация значимых действий всех пользователей в системе



Оповещение о состоянии системы:

- Обновление
- презервное копирование
- работоспособность модулей



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 bcc 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!



