
СИСТЕМА ЗАЩИТЫ ОТ
СПАМА И ФИШИНГА
KAIROS
AV SOFT

ПРОБЛЕМА

Фишинг и спам наиболее простые и востребованные способы проникновения в организацию вирусов и компрометации ее сервисов

Электронная почта является наиболее простым способом проникновения вирусов.

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

Виды угроз

- QR-коды
- Спам письма
- Фишинговые ссылки
- Вредоносные вложения

Цели

- Рассылка вирусов
- Получение личных данных
- Промышленный шпионаж

РЕШЕНИЕ

KAIROS

Система защиты от спама и фишинга, которая анализирует текстовые сообщения, веб-ссылки и вложения в электронных письмах

Технологии

- DKIM, DMARC и SPF
- Динамический анализ
- Антивирусная проверка
- Статический анализ
- Модели машинного обучения
- Внешние аналитические сервисы и базы данных

ТЕХНОЛОГИЯ РАБОТЫ

Источники

Интернет

Почтовый трафик

Объекты

Ссылка

Файл

Текст письма

KAIROS

- Адрес отправителя
- Проверка на спам
- Фишинг
- Антивирусный движок

Сервер

Сервер электронной почты организации

Результат

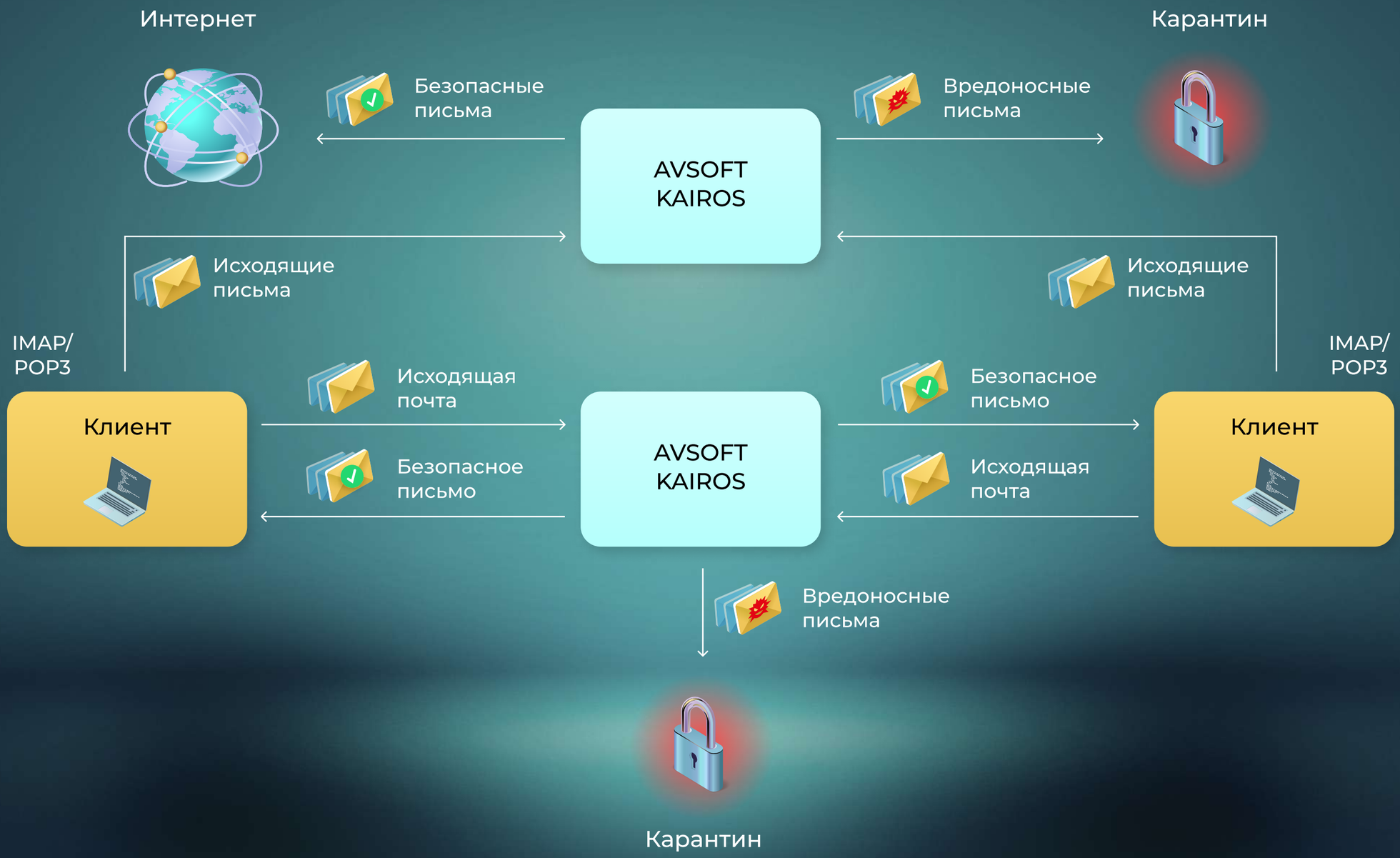
Карантин

Пользователь

SIEM/SOAR

События

ПРОВЕРКА ИСХОДЯЩЕЙ ПОЧТЫ



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

ФИШИНГ И СПАМ

- Целевой фишинг
- Whaling (руководители)
- Прямые и непрямые ссылки
- Скачивание файлов по ссылке
- Ссылки на файловое хранилище

Маски спама

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

ТИПЫ АТАК НА ЭЛЕКТРОННУЮ ПОЧТУ

BACKSCATTER

Письма, которые получают ваши пользователи якобы в ответ на сообщения, которые они никогда не отправляли

ПОЧТОВЫЕ ВЛОЖЕНИЯ

Исполняемый файл, замаскированный под текстовый документ, файл с паролем или запароленный архив, ZIP бомбы и др.

ВЕС-АТАКИ

Фиктивный контрагент, приказ от "руководителя", письмо от "юриста", взлом почты сотрудника

АКТИВНЫЙ КОД

В письмо помещается код, который может выглядеть как кнопка, картинка или вовсе быть невидимым, иногда не обязательно даже нажимать на эту кнопку

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

УНИКАЛЬНАЯ ТЕХНОЛОГИЯ

ИНТЕРНЕТ

Пришла веб-ссылка

AVSOFT KAIROS

Модуль машинного зрения

ПРОВЕРКА В БАЗЕ ДАННЫХ

Скрины публичных сервисов

Скрины корпоративных сервисов

АВТОРИЗАЦИОННЫЕ ДАННЫЕ

- Электронная почта
- Порталы
- Банки и карты
- Формы регистрации данных

Скрин присутствует в базе данных

СРАВНЕНИЕ ДОМЕНОВ В БАЗЕ ДАННЫХ

Скрин нашего сайта (одинаковый)

avsw.ru

Скрин нашего сайта (одинаковый)

РЕЗУЛЬТАТЫ СРАВНЕНИЯ

Домен совпадает → Пользователь

Домен не совпадает → Вырезание ссылки

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

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

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 API интерфейса

Фиксация значимых действий всех пользователей в системе

Оповещение о состоянии системы:
- обновление
- резервное копирование
- работоспособность модулей

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 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!