



KAIROС

СИСТЕМА ЗАЩИТЫ ОТ
СПАМА И ФИШИНГА

ПРОБЛЕМА

Электронная почта является наиболее простым способом осуществления кибератак посредством распространения спама, фишинга и вредоносных вложений

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

ТИПЫ АТАК НА ЭЛЕКТРОННУЮ ПОЧТУ



BACKSCATTER

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



АТАКИ В МОМЕНТ КЛИКА

Содержимое по ссылке появляется после прохождения письмом всех эшелонов проверки в момент клика пользователем

ПОЧТОВЫЙ ШЛЮЗ

KAIROС

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

Запись в реестре отечественного программного обеспечения №3762 от 23.07.2017

ТЕХНОЛОГИИ



Антиспам



Антивирус



Антифишинг



Политики

ПРОВЕРКА ВСЕХ СОСТАВЛЯЮЩИХ ЭЛЕКТРОННОГО ПИСЬМА



Текст писем



Веб-ссылки



Изображения



Вложения

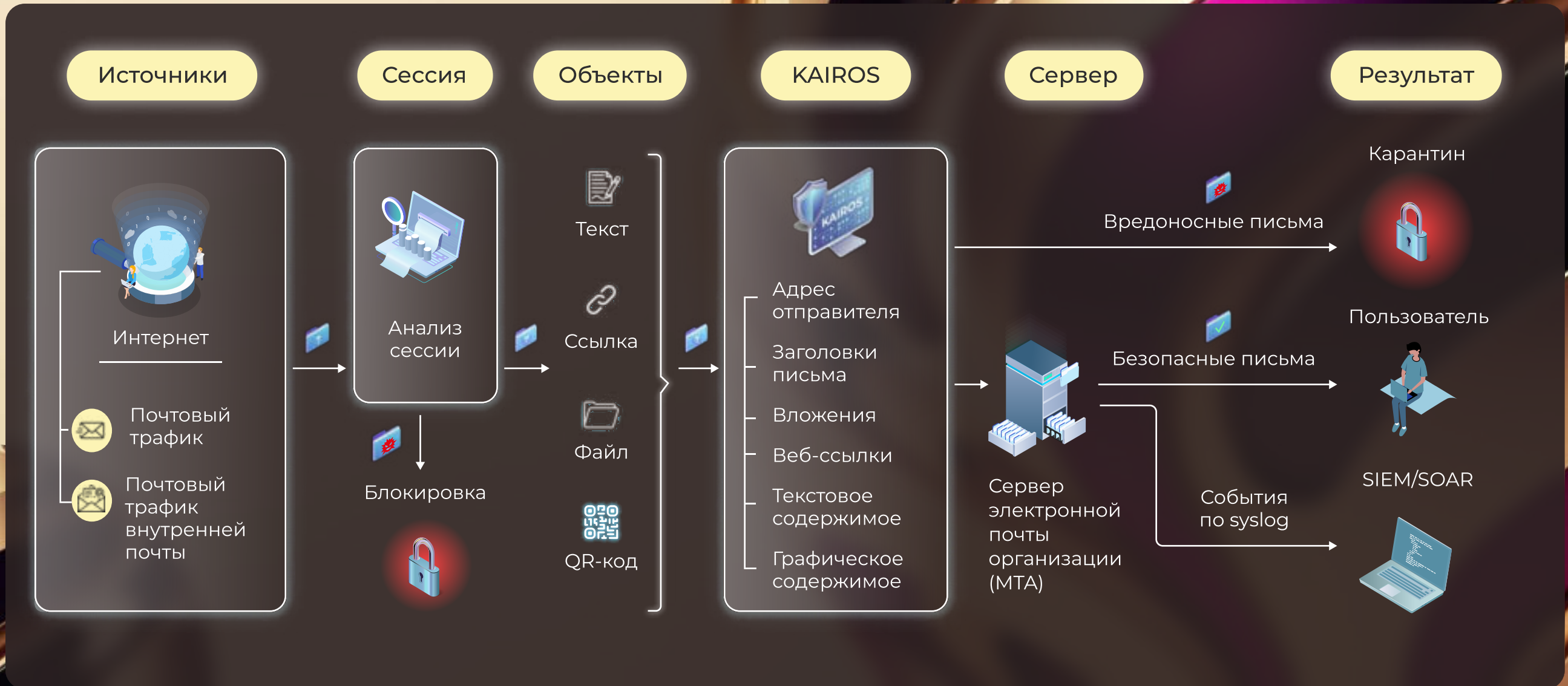


QR-коды



Сессии

ТЕХНОЛОГИЯ РАБОТЫ



ПЕРВИЧНАЯ ПРОВЕРКА

СЕССИОННЫЙ ПРОФИЛЬ

Управление почтовыми сессиями с возможностью тонкой настройки параметров

СЕРЫЙ СПИСОК

Проверка сервера на отношение к рассылке спама с возможностью установить время возобновления сессии

DNSBL

Проверка по черным спискам IP-адресов и доменов на предмет отношения к спаму серверу

АНАЛИЗ ЗАГОЛОВКОВ

Проверка стандартных служебных заголовков на базе гибкой системы аналитик и правил

АНТИСПАМ

СТАНДАРТЫ БЕЗОПАСНОСТИ

DKIM

DMARC

SPF

МАШИННОЕ ОБУЧЕНИЕ

- Использование ансамбля моделей
- Возможность дообучения на данных пользователя



Заголовки



Серый список



Спам листы

- Социальная инженерия
- Реклама и массовая рассылка
- Финансовое мошенничество
- Предотвращение атак сбора каталогов (DNA)
- Защита от спама в уведомлениях о статусе доставки (DSN)

АНТИФИШИНГ

ИНСТРУМЕНТЫ АНАЛИЗА



Динамика переходов по ссылке и коды ответов



Содержимое страницы (анализ кода страницы и js)



Анализ скриншотов веб-страниц



Анализ DNS, сертификата SSL, владельца и др.



Внешние сервисы (Alexa, Whois, PageRank и др)

ТИПЫ УГРОЗ

- Phishing (массовый фишинг)
- Spear Phishing (целевой фишинг)
- Whaling (фишинг на руководство)
- Clone Phishing (фишинг клонов)
- Киберсквоттинг (торговый знак другого лица)
- Тайпсквоттинг (близкие домены)
- DGA (генерация большого количества доменных имен)
- Punycode (алфавитно-цифровые символы)

ТИПЫ ПРОВЕРЯЕМЫХ ССЫЛОК



Прямые и не прямые



Веб-ссылки



IP адреса



На облака и файловые хранилища



С переходами, в том числе с отложенными (meta-refresh)

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, которые хорошо понимают контекст предложения, его настроение и общий смысл



ИЗВЛЕЧЕНИЕ ПРИЗНАКОВ

Для получения вектора признаков используется концепция вложений (embeddings), которая способна 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



УСТАНОВКА И ИНТЕГРАЦИЯ

Система KAIROS может быть интегрирована с внешними системами



Антиспам система по API



Почтовый сервер по SMTP



Система каталогов AD по LDAP



Система сбора событий SIEM по syslog



Песочница и антивирусный мультисканер по API

Система KAIROS поддерживает несколько сценариев развёртывания



Физическая инфраструктура



Виртуальная инфраструктура



Облачная инфраструктура

РЕЖИМЫ 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



ОСОБЕННОСТИ



Уровни угроз с возможностью тонкой кастомизации



Настройка SMTP over TLS для отдельной группы получателей



Дообучение моделей ML на данных корпоративных пользователей



Машинное зрение для анализа изображений, логотипов и QR-кодов



Сбор статистики по нарушению политик безопасности




Возможность задавать до 10 уровней угроз



Настройка правил отдельно для входящей и исходящей почты




КОНТАКТЫ

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

 www.avsw.ru

 office@avsw.ru

 +7 (495) 988-92-25