KAIROS

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

ОБЩАЯ ИНФОРМАЦИЯ

Система KAIROS работает на основе технологий почтового шлюза и систем защиты от спама и фшинга. Ее основная задача — проверка объектов анализа на спам, фишинг, вредоносное программное обеспечение.

Проверка в системе KAIROS включает в себя несколько параллельных исследований множеством инструментов, каждый из которых имеет свой вердикт, окончательное решение принимается по высшему вердикту. По окончании исследования выдается подробный отчет.

Система KAIROS принимает на проверку данные из различных источников:

- Веб-трафик
- Почтовый трафик
- Мессенджеры
- Ручная загрузка
- API интерфейс
- ICAP

Система KAIROS способна анализировать следующие типы данных:

- Атрибуты электронных писем
- Текстовое содержание электронных писем
- Веб-ссылки
- QR коды
- Файлы

УГРОЗЫ

Система KAIROS обеспечивает защиту от следующих видов угроз информационной безопасности:

Спам

Фишинг

Вредоносное программное обеспечение

АНТИСПАМ

Система KAIROS имеет возможность проверять следующие записи сетевого домена:

- DKIM
- DMARK
- SPF

Система KAIROS имеет модели машинного обучения, которые по основным и косвенным признакам выносят самостоятельный вердикт относительно текстового контента электронного письма на предмет его отношения к спаму.

Система KAIROS способна проводить анализ заголовков электронных писем по следующим параметрам:

- Received
- Reply-To
- Received-SPF
- DKIM
- X-Headers
- X-Distribution
- To
- Bcc
- Date
- Message-ID
- X-UIDL

ФИШИНГ

Проверка веб-ссылок на фишинг осуществляется одновременнно в следующих направлениях:

Внешние аналитические источники

Проверка переходов

Модели машинного обучения

Статический анализ

Виды моделей машинного обучения для анализа веб-ссылок на фишинг:

- RandomForest (PHISHING.dill)
- Нейронная сеть (neuro_PHISHING.h5)
- Catboost (model_Cat_*)

Внешние аналитические сервисы:

- XSEO
- PhishTank
- Urlscan
- VirusTotal Domain
- VirusTotal URL

ФАЙЛЫ

Система KAIROS позволяет проверять следующие типы файлов:

- Исполняемые файлы (EXE, ELF, CMD)
- Офисные документы (DOCX, DOTM, XLSX, PPTX, PDF, RTF)
- Мобильные приложения (APK)
- Архивы, включая многотомные и защищенные паролем (ZIP, JAR, RAR, 7Z)
- Скрипты (BAT, SH) и др.
- Почтовые форматы, в том числе EML и MSG.

Проверка файлов осуществляется следующими методами анализа:

- Контрольная сумма
- Антивирусный движок

Система KAIROS обеспечивает распаковку и расшифровку по словарю следующих типов файлов:

Архивов

Файлов

PDF

ПОЛИТИКИ

Система KAIROS позволяет осуществлять настройку следующих типов политик:

- Фильтрация по типам файлов
- SMTP сессии
- Репутация отправителя
- Домены
- Рейтинг получателя
- Спам

Система KAIROS иметь систему очередей с возможностью повышения приоритета проверки для привилигерованной категории и настройки правил проверки для разных групп пользователей.

ИНТЕГРАЦИЯ

Система KAIROS поддерживает интеграцию со следующими типами систем:

- Межсетевой экран
- Мультисканер
- Почтовый шлюз
- SIEM/SOAR
- Active Directory
- Песочница

Система KAIROS поддерживает интеграцию с внешними системами по следующим протоколам:

- SMTP
- IMAP/IMAPS
- REST API
- POP3/POP3S
- ICAP
- SYSLOG

ИНСТАЛЛЯЦИЯ И РЕЖИМЫ ПРОВЕРКИ

Система KAIROS поддерживает следующие варианты установки:

Физический сервер

Виртуальная среда

Облачная среда

Почтовый трафик может проверяться в разных режимах:

- Зеркало
- В перерыве
- Архивная папка
- Протокол REST API

МАШИННОЕ ОБУЧЕНИЕ

Машинное обучение позволяет автоматически обнаруживать спам и фишинг на основе ретроспективного анализа баз данных, накопленных в системе KAIROS. Изучив большое количество образцов модель машинного обучения способна обобщать информацию и обнаруживать новые виды спама и фишинга.

В системе KAIROS для классификации и обработки текстов используются модели на базе новой технологии – трансформеры. Они хорошо понимают контекст предложения, его настроение и общий смысл, что позволяет эффективно идентифицировать спам.

Для получения вектора признаков используется концепция вложений (embeddings), которая способна определять связи между словами, их многозначность, последовательность, преобразование, контекст, частоту употребления.

Система KAIROS позволяет в автоматическом режиме дообучать модули машинного обучения в том числе на данных пользователя.