КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Проактивный подход выявления вредоносных регистраций доменных имен

Вадим Михайлов

Состояние и перспективы развития ИКТ-инфраструктуры 2022

cctld.ru | кц.рф

.RU .РФ

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

План доклада

- Классический подход выявления вредоносных доменных имен
- Проактивные методики выявления вредоносных регистраций
- Сложности реализации
- Сценарии действий
- Примеры исследований и разработок
- Выводы

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Классический подход



КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Проблема



КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Проблема





КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Решение



Решение





Методики

– на основе анализа контактной информации

Методики

– на основе анализа контактной информации



Методики

– на основе анализа контактной информации



+380 XX XXX XXXX

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– на основе анализа контактной информации



+380 XX XXX XXXX

恶意的 意图

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

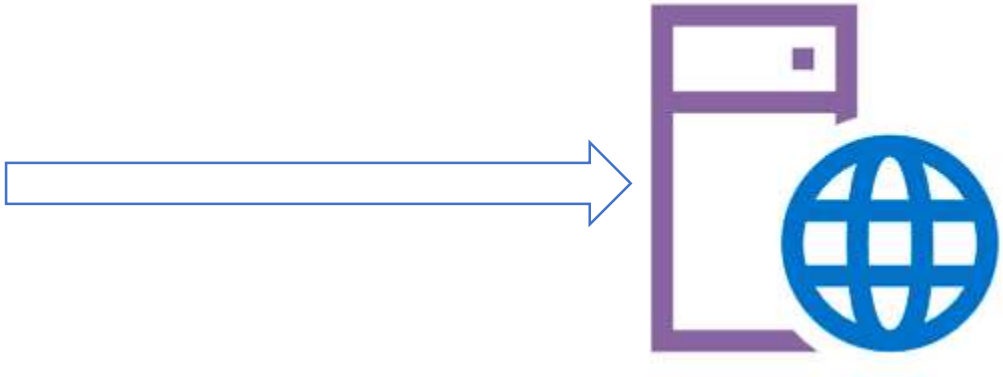
Методики

– на основе анализа параметров делегирования

Методики

– на основе анализа параметров делегирования

IPv4
IPv6



Абьюзоустойчивый хостинг

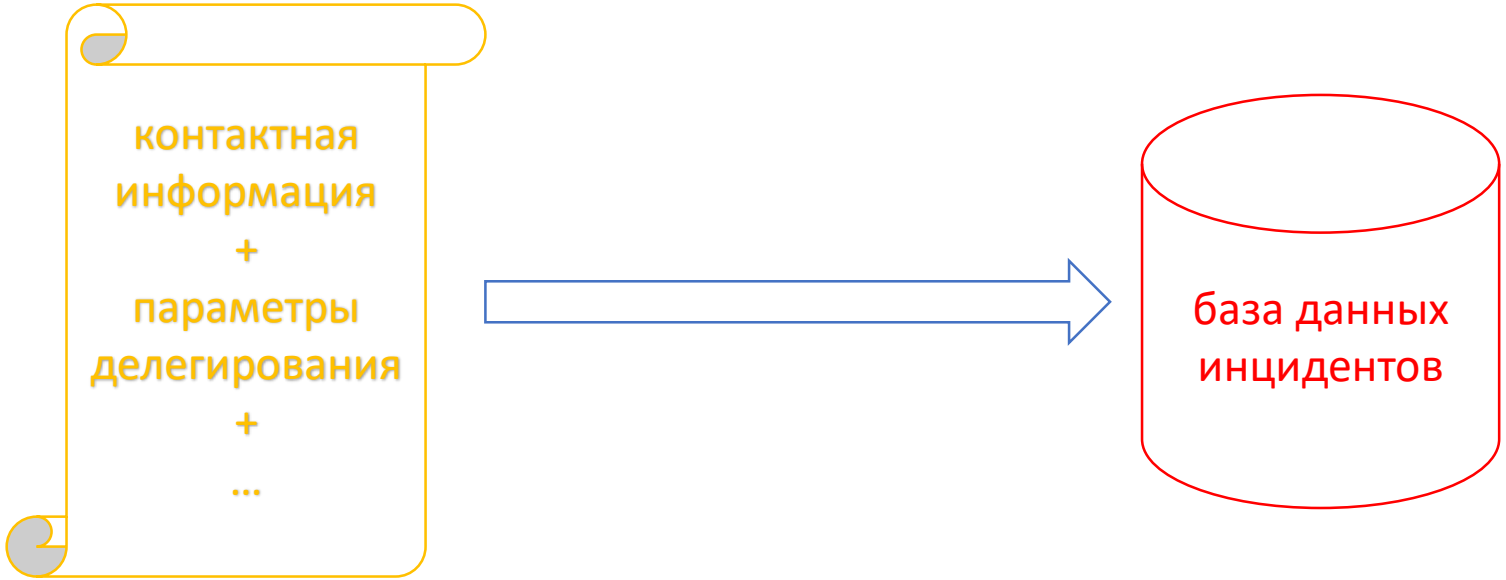
КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– ретроспективный анализ

Методики

– ретроспективный анализ



КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– на основе схожести между существующими и регистрируемыми доменными именами

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– на основе схожести между существующими и регистрируемыми доменными именами

- plati и oplati
- paypal и paypa1
- госуслуги и госуслути

Методики

– на основе схожести между существующими и регистрируемыми доменными именами

строковое расстояние
(Дамерау — Левенштейна)

к	о	т
к	о	д

расстояние = 1

	к	о	т	и	к	
с	к	о	т	и	н	а

расстояние = 3

Методики

– на основе схожести между существующими и регистрируемыми доменными именами

таблицы схожих символов – омоглифов

o	o	идентичны
0	O	высокий
1	l	высокий
l	I	высокий

простые

и	й	средний
е	ё	средний
d	ԁ	высокий
а	ā	средний

с диактрическими символами

w	vv	высокий
m	rn	высокий
ffl	ffl	средний
љ	ль	средний

составные

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– на основе схожести со словарями подозрительных доменных имен

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Методики

– на основе схожести со словарями подозрительных строк

- microzaem, vdolg, credit, perevod, …
- coronavirus, covid, sputnikv, …
- миграция, виза, отсрочка, повестка, …
- + DGA-домены

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сложности

– Большое количество данных

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сложности

- Большое количество данных
- Множество вариантов их сочетания

Сложности

- Большое количество данных
- Множество вариантов их сочетания
- Необходимость подстраивать весовые коэффициенты и пороговое значение

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

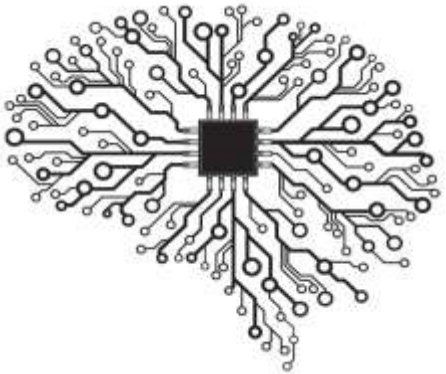
Сложности

- Большое количество данных
- Множество вариантов их сочетания
- Необходимость подстраивать весовые коэффициенты и пороговое значение
- Существенные временные затраты

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сложности

- Большое количество данных
- Множество вариантов их сочетания
- Необходимость подстраивать весовые коэффициенты и пороговое значение
- Существенные временные затраты

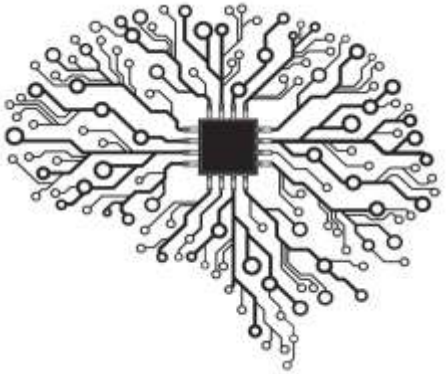


применение алгоритмов машинного обучения

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сложности

- Большое количество данных
- Множество вариантов их сочетания
- Необходимость подстраивать весовые коэффициенты и пороговое значение
- Существенные временные затраты



применение алгоритмов машинного обучения

+

к экспертному анализу

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сценарии

– Отложенная регистрация

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сценарии

- Отложенная регистрация
- Отложенное делегирование

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Сценарии

- Отложенная регистрация
- Отложенное делегирование
- Классическая схема снятия с делегирования

Примеры

- Швейцария, SWITCH, регистратура .ch/.li – внедрение отложенного делегирования с 2021 года

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Примеры

- Швейцария, SWITCH, регистратура .ch/.li – внедрение отложенного делегирования с 2021 года

- Британия, Nominet, регистратура .uk – проект Domain Watch 2021 – блокирование фишинговых доменов при регистрации

Примеры

- Швейцария, SWITCH, регистратура .ch/.li – внедрение отложенного делегирования с 2021 года

- Британия, Nominet, регистратура .uk – проект Domain Watch 2021 – блокирование фишинговых доменов при регистрации

- Координационный центр доменов .RU/.РФ – в 2022 году проведена НИР «Методология определения вероятности противоправного (вредоносного) использования доменных имен в доменах .ru и .рф на основании набора параметров/индикаторов (технических данных), полученных в процессе регистрации доменного имени и его активации (делегировании).»

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Выводы

– «Болезнь легче предупредить, чем лечить»

Гиппократ

Выводы

- «Болезнь легче предупредить, чем лечить»

  Гиппократ

- Развитие ML-технологий позволяют эффективнее работать на опережение

Выводы

- «Болезнь легче предупредить, чем лечить»

  Гиппократ

- Развитие ML-технологий позволяют эффективнее работать на опережение
- Крайне важен обмен данными об инцидентах для обучения алгоритмов

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Выводы

- «Болезнь легче предупредить, чем лечить»

  Гиппократ

- Развитие ML-технологий позволяют эффективнее работать на опережение
- Крайне важен обмен данными об инцидентах для обучения алгоритмов
- Еще предстоит немало исследований

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

СПАСИБО ЗА ВНИМАНИЕ!

Вадим Михайлов

mva@cctld.ru
мва@кц.рф