

Ассоциированные домены

Расследование угроз
и сотрудничество с регистратором

Один инцидент — начало проверки всей связанной инфраструктуры

Наш практический опыт

≈ 1–2 ТЫС.

вредоносных доменов выявлено
в совместной работе с регистратором

В отдельных аккаунтах — десятки и сотни других вредоносных доменов

Предмет обсуждения: DNS Abuse

Фишинг

Похищение данных через обман

Вредоносное ПО

Распространение и работа вредоносных программ

Ботнеты

Инфраструктура управления заражёнными устройствами

Фарминг

Перенаправление через подмену разрешения имён

Спам

Когда служит доставке перечисленных угроз

Три группы доказательств связи

/ 01

Данные регистратора

Аккаунт клиента
Контакты и заказы

/ 02

Контент и функции

Зеркала и код
Получатель данных

/ 03

Инфраструктура и поведение

DNS и сертификаты
Синхронные изменения

Связь доменов и участие в атаке — отдельные оценки

Контент как доказательство связи

/ 01 **Общий получатель данных**

Формы отправляют данные в один выделенный обработчик

/ 02 **Общие элементы кампании**

Специфический код, идентификаторы и цепочки перенаправлений

Одинаковый шаблон сам по себе не устанавливает одного оператора

Что добавляет регистратор

Аккаунт конечного клиента

Контакты и платежи
Заказы и время регистрации
История управления

Исследователь передаёт признаки кампании.
Регистратор проверяет связи по данным клиента.

Инфраструктура и время

/ 01 Редкие технические совпадения

DNS, сертификаты, выделенные серверы и конфигурации C2

/ 02 Согласованные изменения

Серии регистраций, одновременный запуск, смена DNS

/ 03 Резерв кампании

Новый домен принимает функцию отключённого ресурса

Источники для расследования

Регистрационные сведения

RDAP + данные регистратора

История инфраструктуры

Passive DNS / DomainTools

Сертификаты и серверы

Censys / Certificate Transparency

Страницы и переходы

urlscan / анализ сетевых обращений

Вредоносное ПО

VirusTotal / анализ образцов

Что передавать в abuse-репорте

/ 01 **Объект и время**

Домен, точный URL, тип abuse, время наблюдения

/ 02 **Доказательства инцидента**

Содержимое, сетевые обращения, технические артефакты

/ 03 **Признаки для расширения проверки**

Связанные домены, получатель данных, идентификаторы кампании

Совместная работа с кампанией

/ 01

Подтвердить
инцидент

Исследователь



/ 02

Найти связанные
регистрации

Регистратор



/ 03

Проверить группу
и принять меры

Совместная работа

Обратная связь и наблюдение за восстановлением инфраструктуры

Наша позиция

**Подтверждённый инцидент
должен запускать проверку
связанных доменов**

Доказательства исследователя + данные регистратора