Разбор задач HackTheBox по OSINT

ДОКЛАДЧИК: (Сергей Сталь/noname)

ДИСКЛЕЙМЕР

18+

Автор материала не несет ответственности за действия совершенные слушателями.

Инфорформация предоставлена исключительно в ознакомительных целях.

Разбор задачи HackTheBox. Прохождение лаборатории OSINT (уровень: easy)

Получить требуемый ответ возможно разными способами.

Главное правильно задавай вопросы и выбрать нужный инструмент

Условия задачи

CHALLENGE DESCRIPTION

Customers of ***secure-startup.com*** *have been recieving some very convincing phishing emails, can you figure out why?*

Что будем искать

Для решения нам потребуется найти информацию, спрятанную в домене secure-startup.com

DKIM (DomainKeys Identified Mail) — технология проверки электронной почты, с помощью которой можно вычислить поддельные письма. DKIM добавляет в письмо цифровую подпись. Благодаря ей почтовые провайдеры могут проверить, что сообщение отправлено именно с указанного домена.

Как работает DKIM?

DKIM делится на 2 части: то, что происходит на сервере-отправителе, и то, что происходит на сервере-получателе. Всем процессом заправляют приватный и публичный ключ.

Приватный ключ (private key) – секретный уникальный код, который хранится на сервере или под надзором email сервиса.

На сервере-отправителе.

При отправке каждое сообщение подписывается цифровой подписью, используя приватный ключ DKIM.

В графе должно находиться имя домена-отправителя: по нему происходит идентификация.

Нижняя строка выделена квадратиком

Test system Dkim

Входящие x

Евгений support.estismail@yandex.ru через estismailer.com 13:40 (3 мин. назад)

кому: мне

от:	**Евгений** <support.estismail@yandex.ru>
Кому:	support@estismail.com
дата:	10 августа 2015 г., 13:40
тема:	Test system Dkim
список рассылки:	estismail-2015-10-12633 Фильтровать письма из этого списка рассылки
отправлено через:	estismailer.com
подписан:	estismailer.com

...por
...nostrud

... fugiat nulla
...fficia

...ылки. Если

Вы не желаете больше получать письма этой рассылки, Вы можете отписаться от неё кликнув на ссылку:

Отписаться от рассылки

Письмо отправлено сервисом Estismail.com

Вы получили это письмо, так как подписали емейл support@estismail.com на рассылки от Евгений на странице подписки.

IP-адрес: 93.74.140.206, время подписки: 2015-08-10 13:07.

Получающий сервер начинает проверку входящего email с поля «DKIM-подпись» в заголовке сообщения. Он анализирует:

Версию DKIM, которую использовал отправитель;

Соответствие домена отправителя значению, указанному в подписи;

Значение тега h= (т.е. от кого пришло письмо).

Затем делает запрос в своеобразную библиотеку доменных имен – DNS: подлинный ли домен отправителя?

Ответ положительный – email не меняется и идет дальше в почтовый ящик получателя. Если нет – отправляется в СПАМ.

Как работает *SPF*?

SPF (Sender Policy Framework) — txt запись со списком IP-адресов, которым сайт (домен) доверяет отправку писем от своего имени. SPF хранится на домене и ее запрашивает сервер получателя, чтобы определить, доставлять письмо во «Входящие» или в «Спам».

Как SPF защищает домен:

При получении письма сервер получателя смотрит на поле «с какого домена».

Сервер получателя обращается к домену напрямую и смотрит список IP-адресов, которым он доверяет отправку писем (это и есть SPF).

Сервер получателя сравнивает IP-отправителя с IP-списком в SPF. Если IP-адреса не совпадают, он блокирует письмо.

Как работает *DMARC*?

DMARC – Domain-based Message Authentication, Reporting and Conformance (аутентификация сообщений, предоставление отчетов и проверка соответствия на базе доменного имени). Это относительно новая технология, призванная уменьшить количество подделок сообщений электронной почты, снизить количество фишинговых писем и способствовать борьбе со спамом.

Автор создает и отправляет E-mail

Отправляющий SMTP-сервер добавляет подпись DKIM

E-mail доставляется получателю

ОТПРАВИТЕЛЬ

ПОЛУЧАТЕЛЬ

«Черный список» IP, Rate limit, и т.д.

Стандартные проверочные тесты

Проверка и применение DMARC политики отправителя

Получение подтвержденных DKIM доменов

Получение «Envelop From» через SPF

Применение соответствующей политики DMARC

Антиспам-фильтры и т.д.

Стандартная обработка

В доставку

Карантин

Отчеты об ошибках отправляются отправителю

Обновление периодического агрегированного отчета для отправки отправителю

к нам приходит письмо, например, на почтовый сервер от Google.

Нам требуется понять, какую информацию нам можно изъять из электронного письма?

Берем письмо и нажимаем «Показать оригинал»

Показываю на примере:

Электронный чек по заказу

Входящие ×

Ozon <noreply@ozon.ru> Отказаться от рассылки
кому: мне

OZON

Ваш электронный чек

По заказу [redacted] от 30.12.2021 сформирован
чеки хранятся в Личном кабинете в разделе "Электро

Команда Ozon

Кассовый чек [redacted]

30.12.2021

- Ответить
- Переслать
- Фильтровать похожие письма
- Печать
- Удалить это письмо
- Заблокировать отправителя "Ozon"
- В спам!
- Сообщить о фишинге
- Показать оригинал
- Перевести сообщение
- Скачать сообщение
- Отметить как непрочитанное

Исходное сообщение

Идентификатор сообщения	<20211230160629.0.20211230160629_pe_@3350665033578233536.ozon.pegate>
Создано:	30 декабря 2021 г., 16:06 (доставлено через 3 секунды)
От:	Ozon <noreply@ozon.ru>
Кому:	@gmail.com
Тема:	Электронный чек по заказу
SPF:	PASS с IP-адресом 185.235.29.24. Подробнее…
DKIM:	'PASS', домен ozon.ru Подробнее…
DMARC:	'PASS' Подробнее…

По данным значениям будем разбирать домен. Для этого воспользуемся ресурсом ***mxtoolbox.com****.*

Давайте посмотрим, какую информацию мы можем получить по домену secure-startup.com по SPF

SuperTool | MX Lookup | Blacklists | DMARC | Diagnostics | Email Heal

SuperTool Beta7

secure-startup.com

SPF Record Lookup

spf:secure-startup.com

Find Problems

```
v=spf1 a mx ?all - HTB{RIP_SPF_Always_2nd
```

SuperTool | MX Lookup | Blacklists | DMARC | Diagnostics | E

SuperTool Beta7

secure-startup.com

DMARC Lookup

dmarc:secure-startup.com

Find Problems

v=DMARC1;p=none;_F1dd13_2_DMARC}

Флаг найден

HTB{RIP_SPF_Always_2nd_F1ddl3_2_DMARC}

Ну что пора поговорить о более сложных и интересных задачах

Разбор задачи с ресурса HackTheBox

На поиски Сары. Продолжаем разбор лаборатории OSINT (Уровень: Easy)

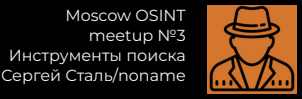
We are looking for Sara Medson Cruz's last location, where she left a message. We need to find out what this message is! We only have her email: **saramedsoncruz@gmail.com**

В этот раз задачка найти Сару по почте **saramedsoncruz@gmail.com** и по ее последним отзывам.

Нам требуется найти информацию, поэтому пишем в Google
Osint: “найти локацию по емайл”.

Но только на английском! Так больше вариантов найти нужное решение.

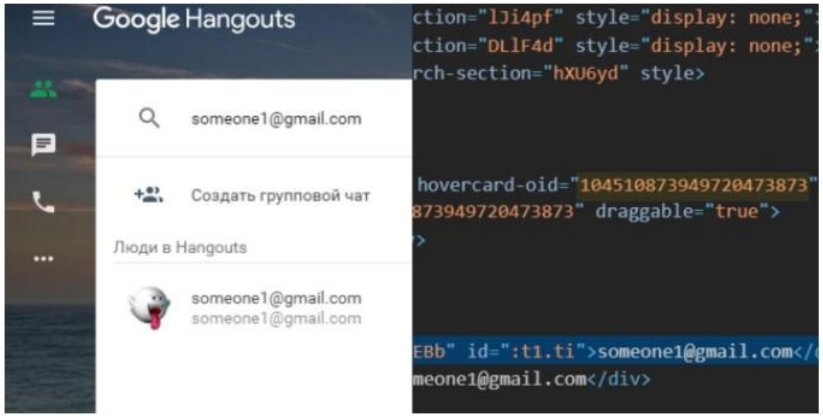
osint find location using email address



Posted by u/810000000400028195 1 year ago

41

How to find user's reviews on Google Maps by Gmail address?



Updated Google ID search method by Gmail address (Old method with contacts is fixed)

1. open hangouts.google.com on your PC and click on your contacts in the left corner.
2. Click on create a chat and enter the gmail address you want in the search.

Right-click on the name of the account and select Inspect.

4. In the developer tools find the line with `hovercard-oid`

5. After this phrase is an ID of 21 digits long, copy this ID

Using Google ID

1. https://get.google.com/albumarchive/GoogleID - replace GoogleID with the numbers you copied, find your account's picture album.
2. https://www.google.com/maps/contrib/GoogleID - replace GoogleID with the numbers you copied, find your Google Maps account.

Updated Google ID search method by Gmail address (Old method with contacts is fixed)

1. open hangouts.google.com on your PC and click on your contacts in the left corner.
2. Click on create a chat and enter the gmail address you want in the search.
3. Right-click on the name of the account and select Inspect.
4. In the developer tools find the line with hovercard-oid
5. After this phrase is an ID of 21 digits long, copy this ID

Using Google ID

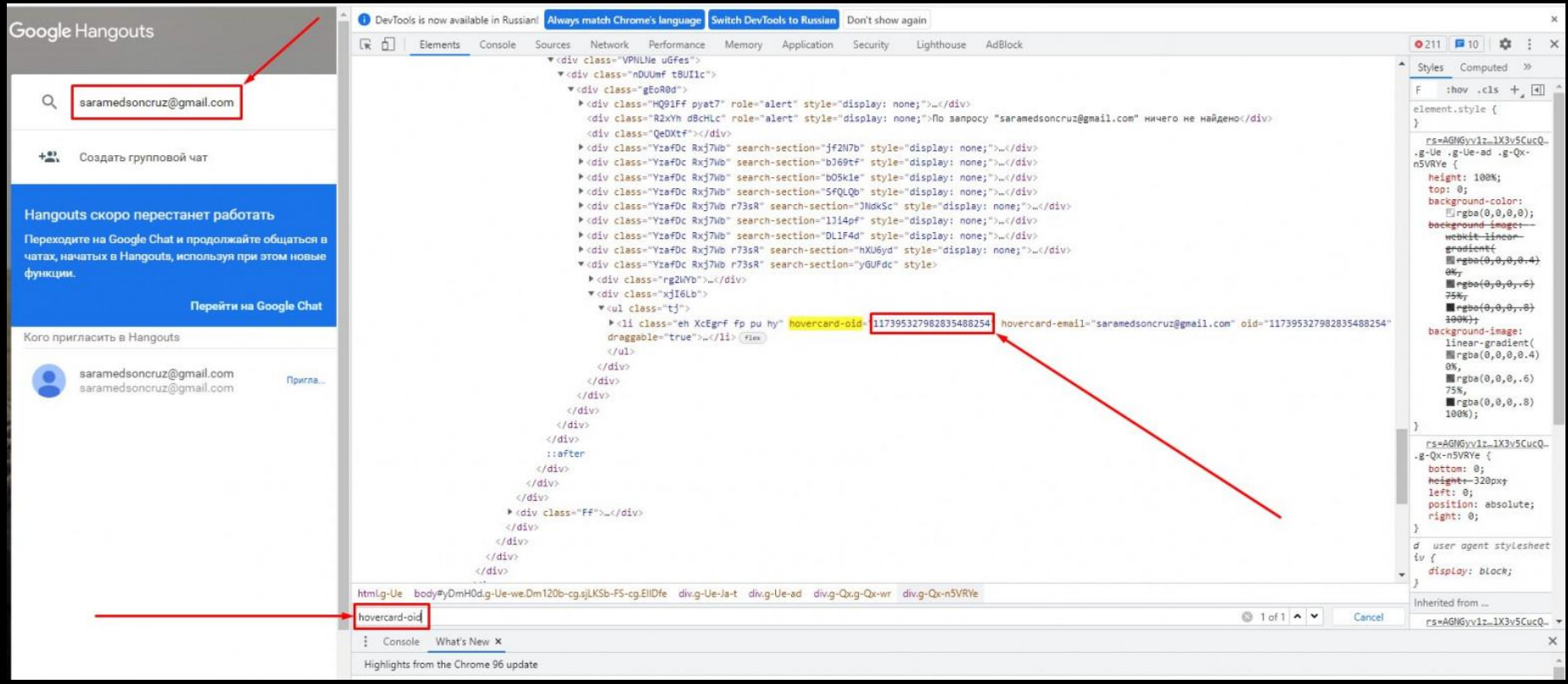
https://get.google.com/albumarchive/GoogleID - replace GoogleID with the numbers you copied, find your account's picture album.

https://www.google.com/maps/contrib/GoogleID - replace GoogleID with the numbers you copied, find your Google Maps account.

Перейдем к поиску флага.

Стряхиваем пыль тысячелетий с Hangouts и создаем там встречу с Сарой.

Начинаем просматривать код. Нам требуется найти ID.

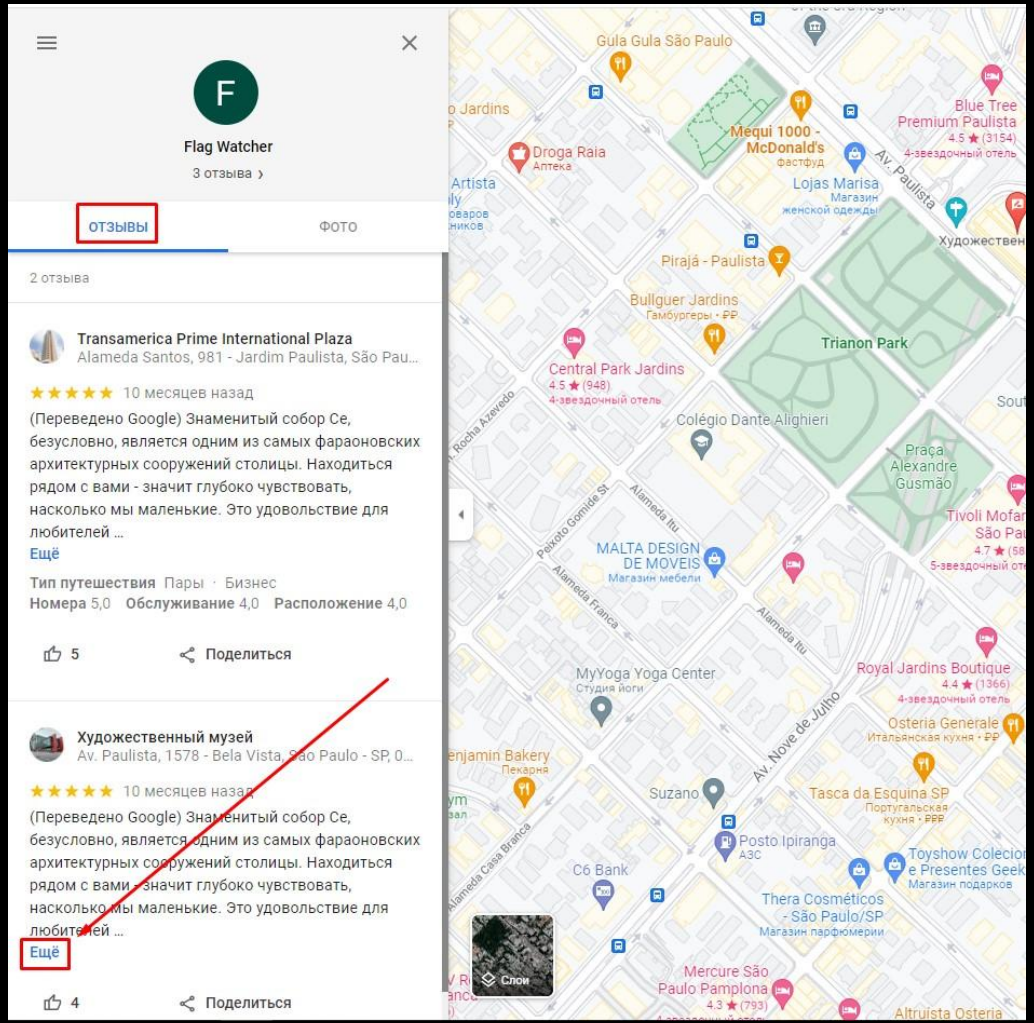

Google Hangouts
saramedsoncruz@gmail.com
Создать групповой чат
Hangouts скоро перестанет работать
Переходите на Google Chat и продолжайте общаться в чатах, начатых в Hangouts, используя при этом новые функции.
Перейти на Google Chat
Кого пригласить в Hangouts
saramedsoncruz@gmail.com
saramedsoncruz@gmail.com
Пригла...
DevTools is now available in Russian!
Always match Chrome's language
Switch DevTools to Russian
Don't show again
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
hovercard-oid="117395327982835488254"
hovercard-email="saramedsoncruz@gmail.com"
hovercard-oid
1 of 1
Cancel
Console
What's New
Highlights from the Chrome 96 update

Заходим по ссылке
https://www.google.com/maps/contrib/GoogleID

Вместо **GoogleID** требуется вписать параметр который мы нашли.

Переходим по сформированной нами ссылке в отзывы.

https://www.google.com/maps/contrib/117395327982835488254

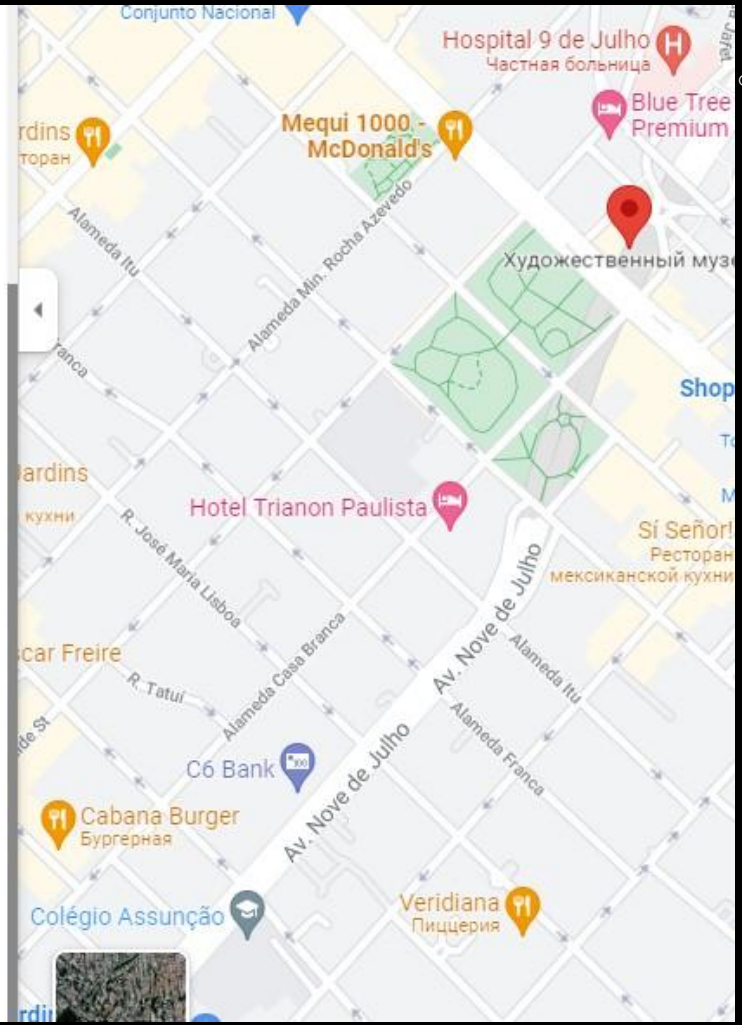

F
Flag Watcher
3 отзыва ›
ОТЗЫВЫ
ФОТО
2 отзыва
Transamerica Prime International Plaza
Alameda Santos, 981 - Jardim Paulista, São Pau...
10 месяцев назад
(Переведено Google) Знаменитый собор Се, безусловно, является одним из самых фараоновских архитектурных сооружений столицы. Находиться рядом с вами - значит глубоко чувствовать, насколько мы маленькие. Это удовольствие для любителей ...
Ещё
Тип путешествия Пары · Бизнес
Номера 5,0 Обслуживание 4,0 Расположение 4,0
5
Поделиться
Художественный музей
Av. Paulista, 1578 - Bela Vista, São Paulo - SP, 0...
10 месяцев назад
(Переведено Google) Знаменитый собор Се, безусловно, является одним из самых фараоновских архитектурных сооружений столицы. Находиться рядом с вами - значит глубоко чувствовать, насколько мы маленькие. Это удовольствие для любителей ...
Ещё
4
Поделиться
Gula Gula São Paulo
Droga Raia
Аптека
Mequi 1000 - McDonald's
фастфуд
Blue Tree Premium Paulista
4.5 (3154)
4-звездочный отель
Av. Paulista
Lojas Marisa
Магазин женской одежды
Pirajá - Paulista
Bullguer Jardins
Гамбургеры · ₽₽
Trianon Park
Central Park Jardins
4.5 (948)
4-звездочный отель
Colégio Dante Alighieri
Praça Alexandre Gusmão
MALTA DESIGN DE MOVEIS
Магазин мебели
Alameda Itu
Alameda Franca
MyYoga Yoga Center
Студия йоги
Royal Jardins Boutique
4.4 (1366)
4-звездочный отель
Osteria Generale
Итальянская кухня · ₽₽
Av. Nove de Julho
Suzano
Tasca da Esquina SP
Португальская кухня · ₽₽₽
Posto Ipiranga
АЗС
C6 Bank
Thera Cosméticos - São Paulo/SP
Магазин парфюмерии
Mercure São Paulo Pamplona
4.3 (793)
Слои

A famosa Catedral da Sé é de longe uma das mais faraônicas estruturas arquitetônicas presentes na capital. Estar ao seu lado é sentir de forma intensa o quanto somos pequenos. É um delírio para apreciadores de construções religiosas. Por fora ela é incrível, por dentro é ainda mais majestosa! Lustres enormes, pilares gigantescos e um clima levemente fúnebre. É um ponto turístico indispensável para todos os públicos, sejam religiosos ou ateus.

E claro, é até irônico ver que diante de tamanha riqueza existam centenas de pessoas mendigando o pão. A praça da Sé, onde fica a igreja, é repleta de pessoas em situação de vulnerabilidade social, não se espante se for abordado ou abordada por uma horda de pessoas lhe pedindo trocados, mas cuidado, nem sempre se trata apenas de "pedir", infelizmente há criminosos que adoram se aproveitar daquele turista distraído fazendo fotos ou mesmo daquela pessoa bondosa que vai abrir sua carteira para doar um trocado. Todo cuidado é pouco.

.
.
.

HTB{i_W4S_D_I_S_c_O_v_3_R_3_D}



А теперь давайте поговорим о чем то более веселом!

Давайте я подкину вам ресурс для решения задач

https://tryhackme.com/

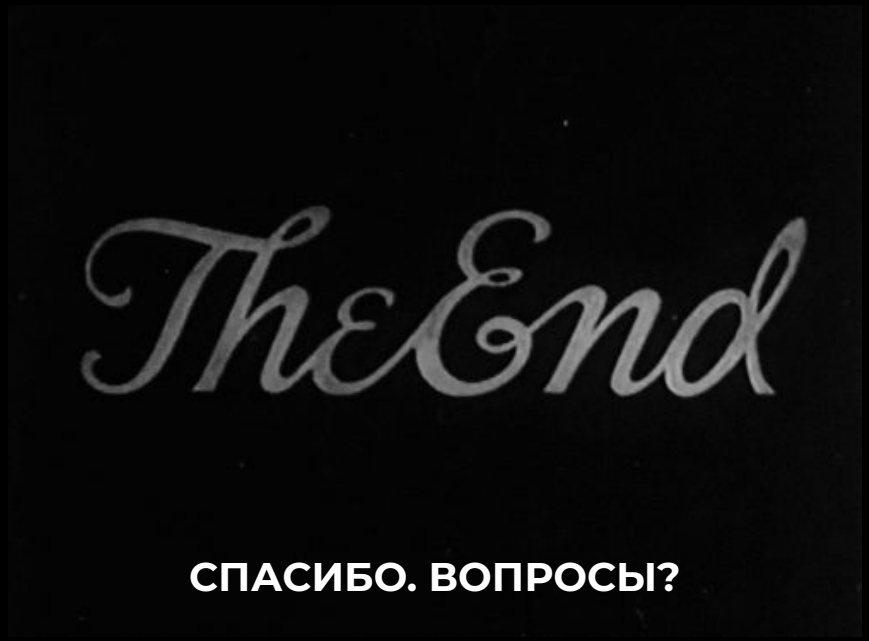
Контакты

Сергей Сталь
Эксперт по информационной безопасности

Мой телеграмм @Sergey646
канал @infobase999

Вопросы?

Если что пишите в телеграмм



СПАСИБО. ВОПРОСЫ?