Лабораторная работа №1

Сбор информации о цели атаки

Выполнили: Завьялова В.В, Ким С.Е, Казачкова О.В.

Группа: Б9118-09.03.04прогин(2).

Цель работы: выявление информации о компании и ее сотрудниках для дальнейшего определения вектора атаки.

Цель атаки: Zapier

Критерии выбора:

1. Репозиторий на GitHub – https://github.com/zapier
2. Профиль на LinkedIn – https://www.linkedin.com/company/zapier
3. Программа Bug Bounty – hackerone.com/zapier-old

Поиск информации осуществлялся в рамках методологии OSINT и с учетом 272 и 273 УК РФ.

Сбор информации о компании

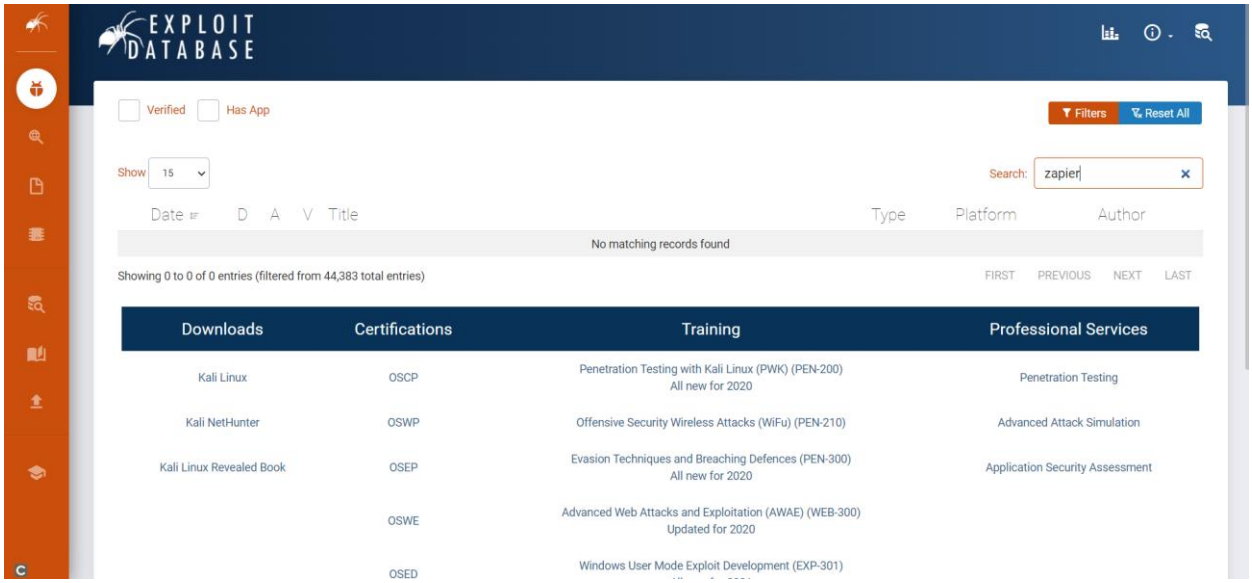
Zapier – это ПО (и одноименная компания), которое позволяет конечным пользователям интегрировать используемые ими веб-приложения. Zapier базируется в Калифорнии. Штаб Zapier состоит из 350 сотрудников, которые работают в США и 23 других странах [1].

Дата основания: 2011 г., Колумбия, Миссури, США.

Адрес: 548 Market St. #62411, San Francisco, California, 94104, United States.

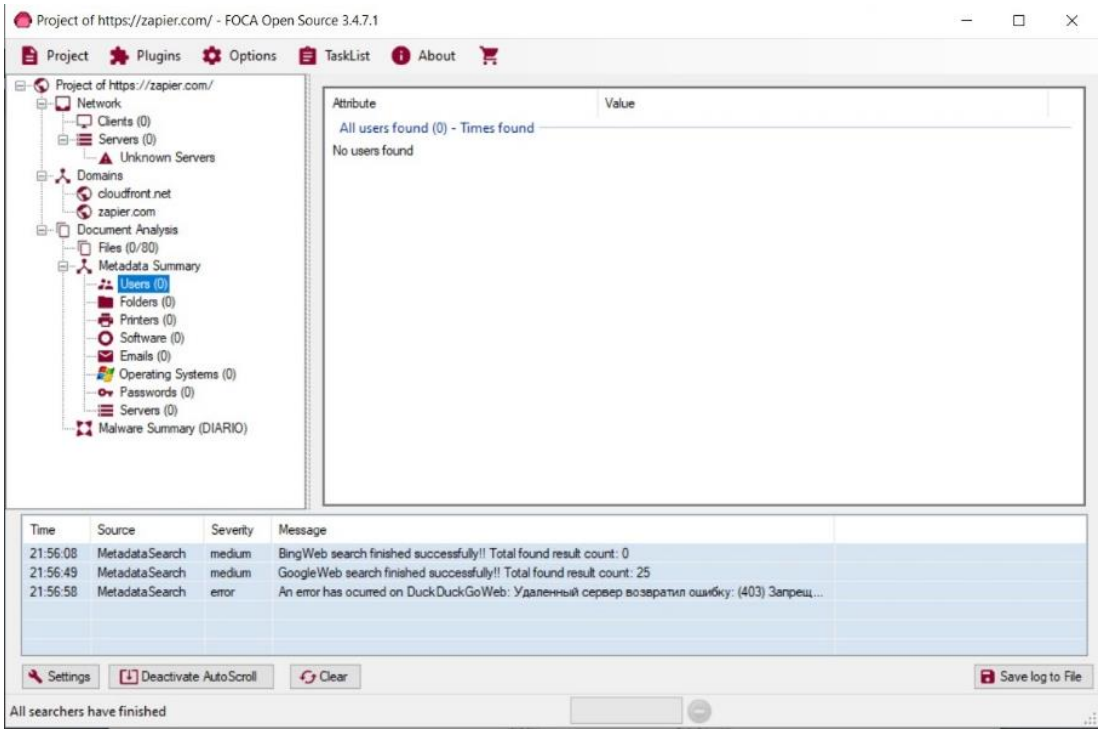
При поиске информации о компании были использованы следующие инструменты и ресурсы:

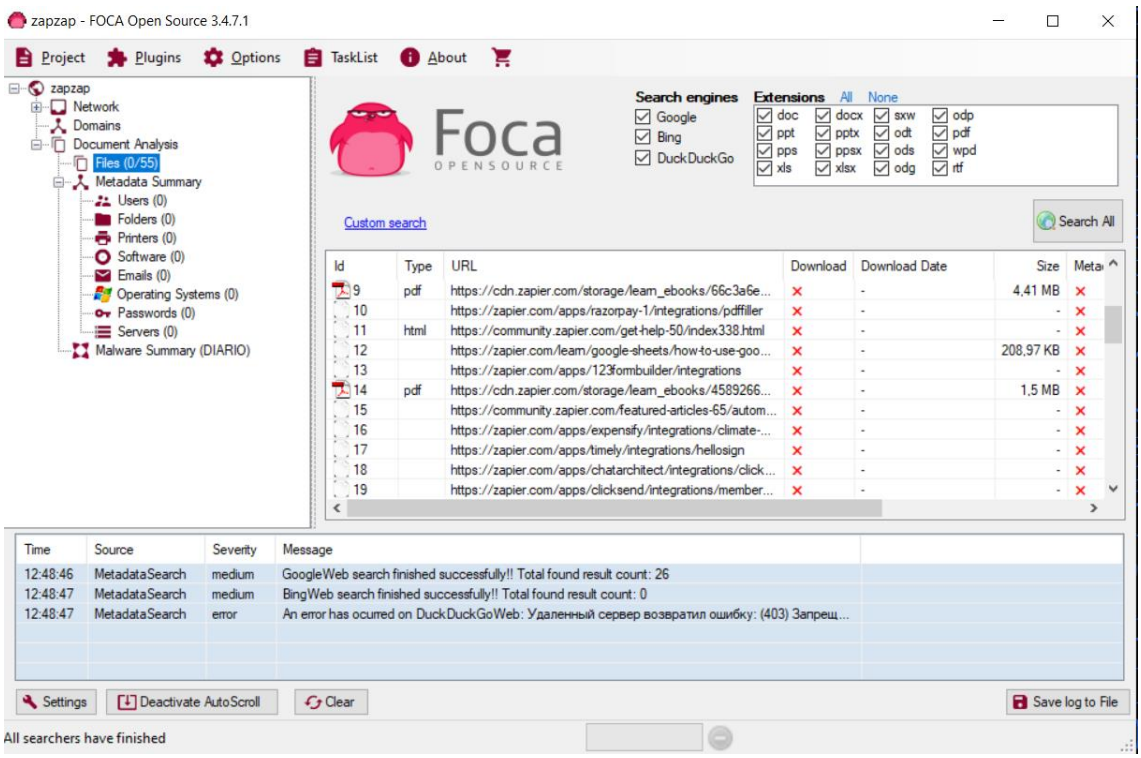
1. Google dork - exploit-db.com/google-hacking-database



Поиск по данному ресурсу не принес полезной информации. Сливов БД Zapier, а также какой-либо “juicy” информации обнаружено не было.

2. github.com/ElevenPaths/FOCA





По результатам разведки при помощи Foca были найдены различные документы компании (обучающие книги, шаблоны презентаций, шаблоны лого и оформления документов и т.п.). Какой-либо информации о серверах, авторах документов, e-mail, ПО найдено не было.

3. osintframework.com

Были использованы следующие сайты для поиска информации о некоторых сотрудниках Zapier:

https://centralops.net/co/DomainDossier.aspx

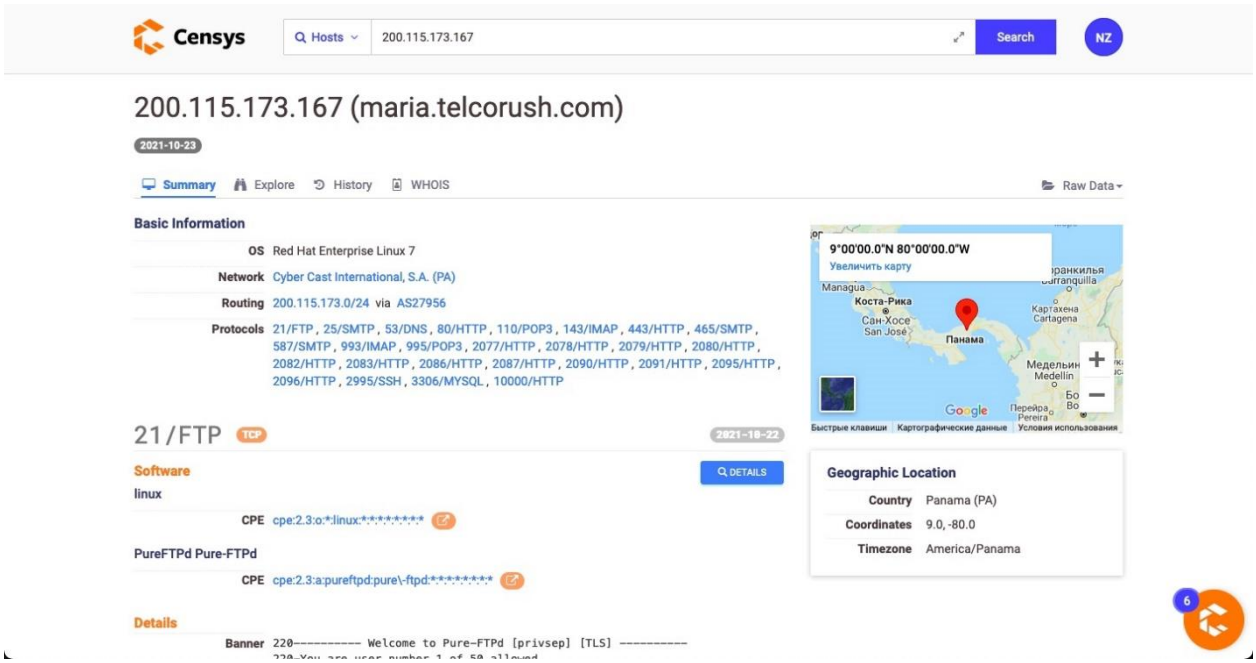
https://haveibeenpwned.com/

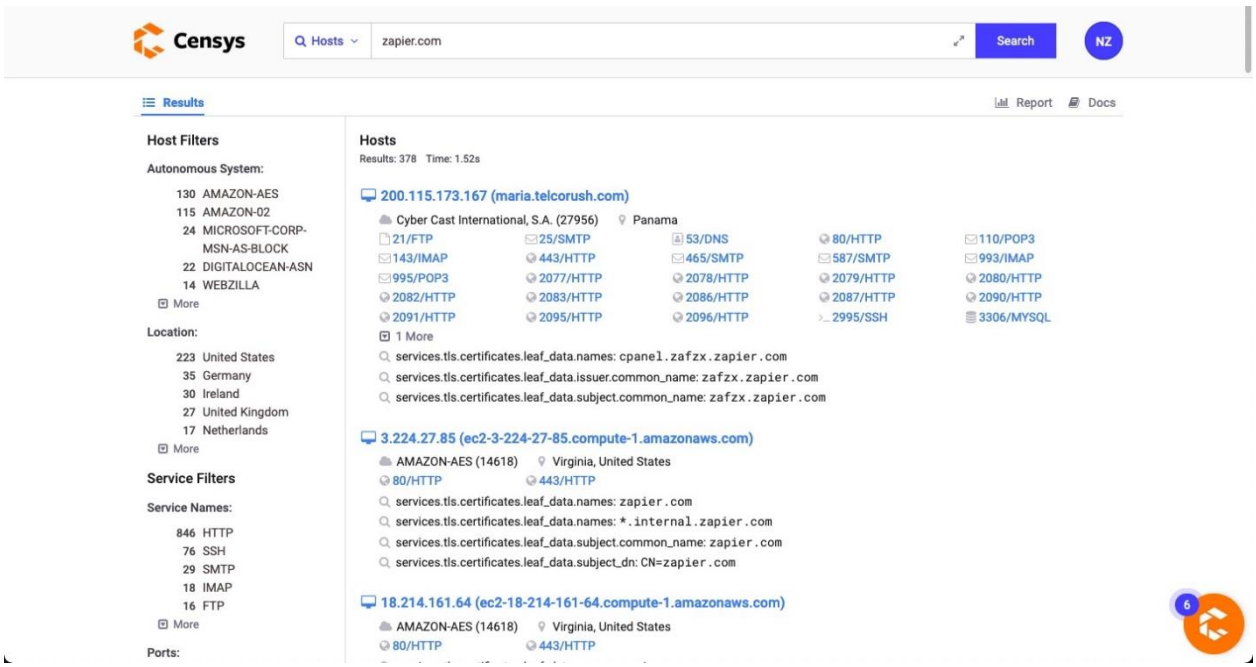
https://whois.domaintools.com/

https://emailrep.io/

С полученной информацией можно ознакомиться в разделе Данные о сотрудниках.

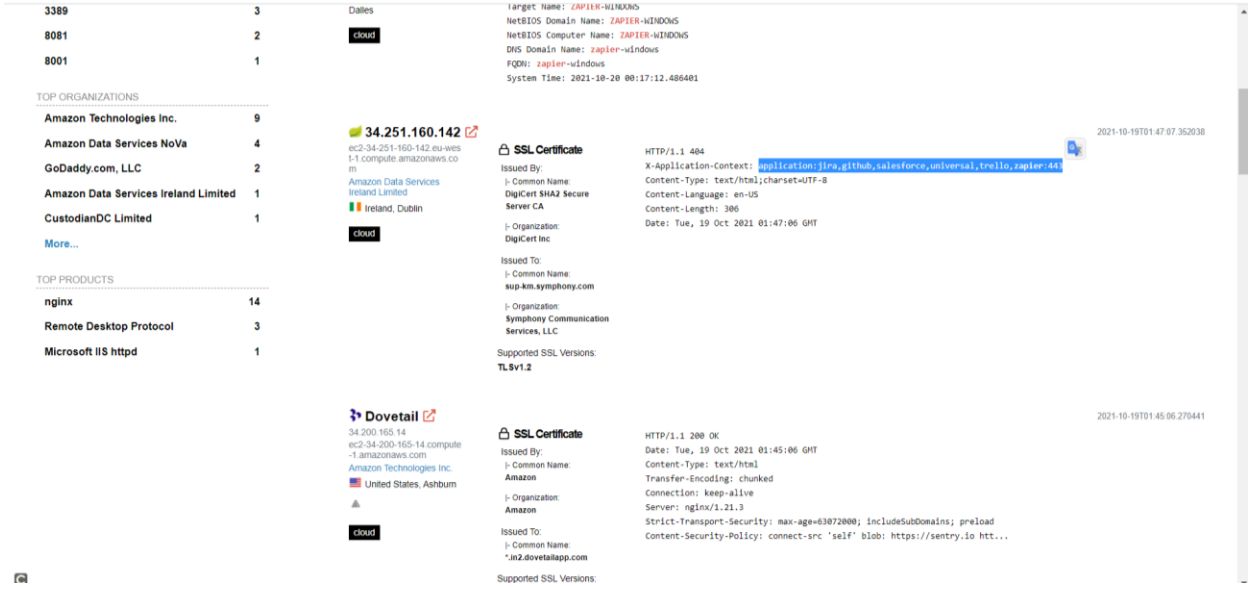
4. censys.io

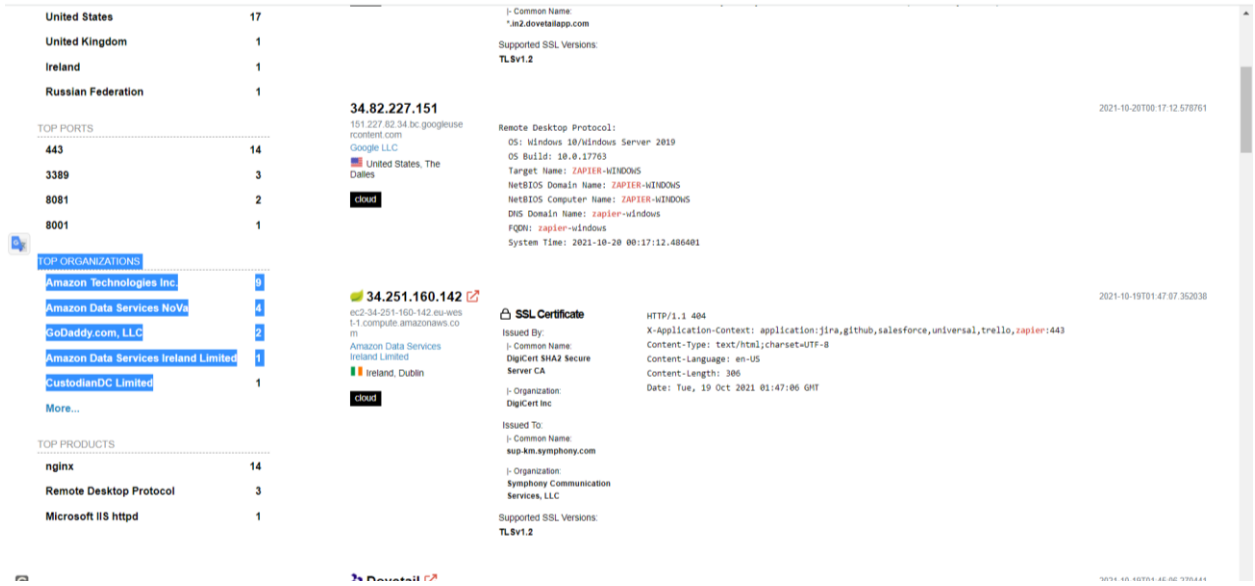




Разведка при помощи censys показала адреса доменов и связанные открытые порты. Скорее всего это компании, пользующиеся ПО, которое предоставляет Zapier, и размещающие их у себя на арендуемых серверах Amazon.

5. shodan.io

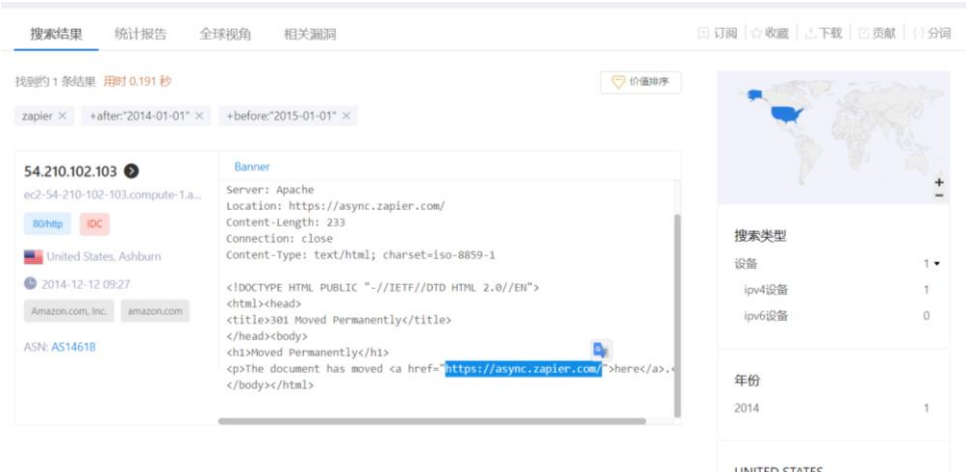




Аналогично censys, shodan позволил получить информацию об адресах доменов пользователей компании, связанных с Zapier.

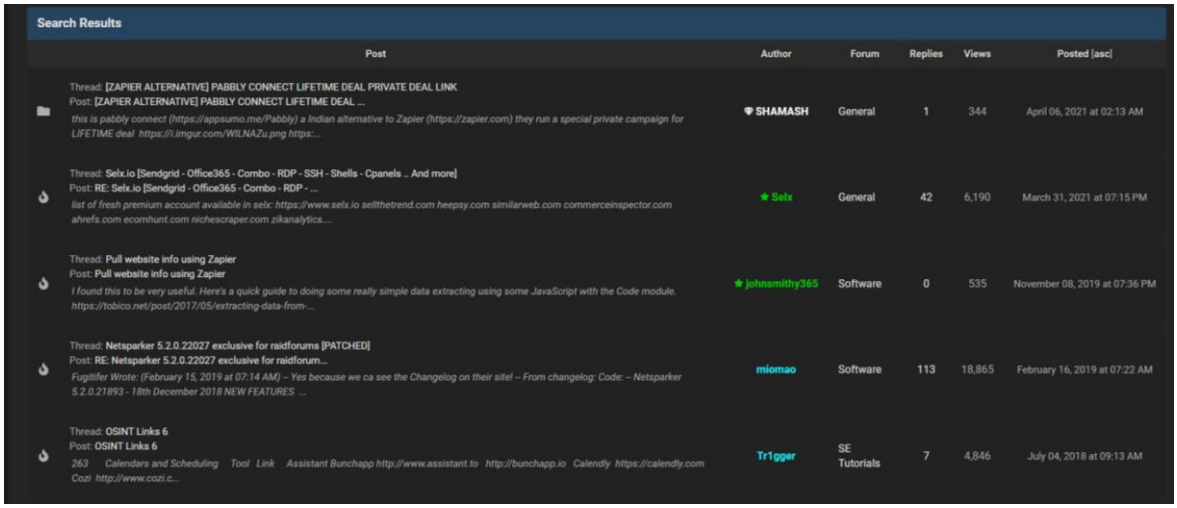
6. zoomeye.org

По результатам исследований были найдены адреса доменов и открытые порты, предоставляющие доступ к данным о клиентах Zapier, которые размещают данные на собственных серверах (appDefinitionName=“integration Zapier”).



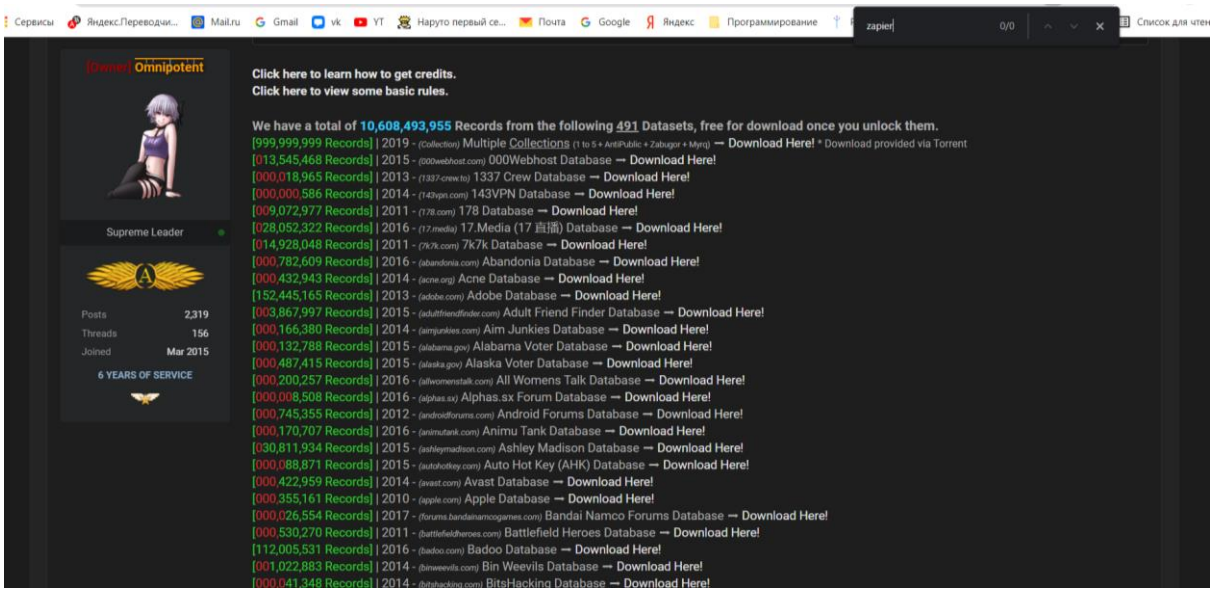
Также, после фильтрации полученной информации по годам (в данном примере взят 2015 г.), был обнаружен сайт https://async.zapier.com/. В ходе изучения, было выяснено, что Async.zapier – внутренний инструмент Zapier (специально созданный), используемый для связи в компании, наподобие внутренней системы блогов. Доступ возможен через почту google, но существует внутренняя аутентификация (проверка) на принадлежность gmail’a компании Zapier.

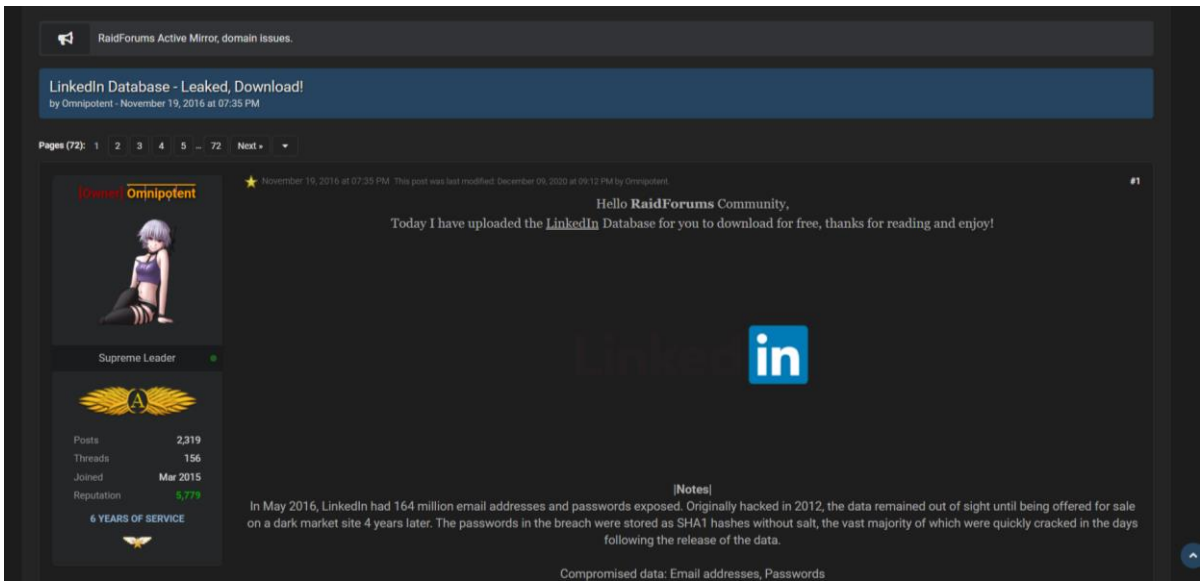
7. raidforums.com



По результатам исследования были обнаружены результаты, которые не имели весомого вклада в расследование: установка более дешевого варианта Zapier от индийских разработчиков; пример JS скрипта для получения информации о веб-сайте с помощью Zapier (легально); т.п.

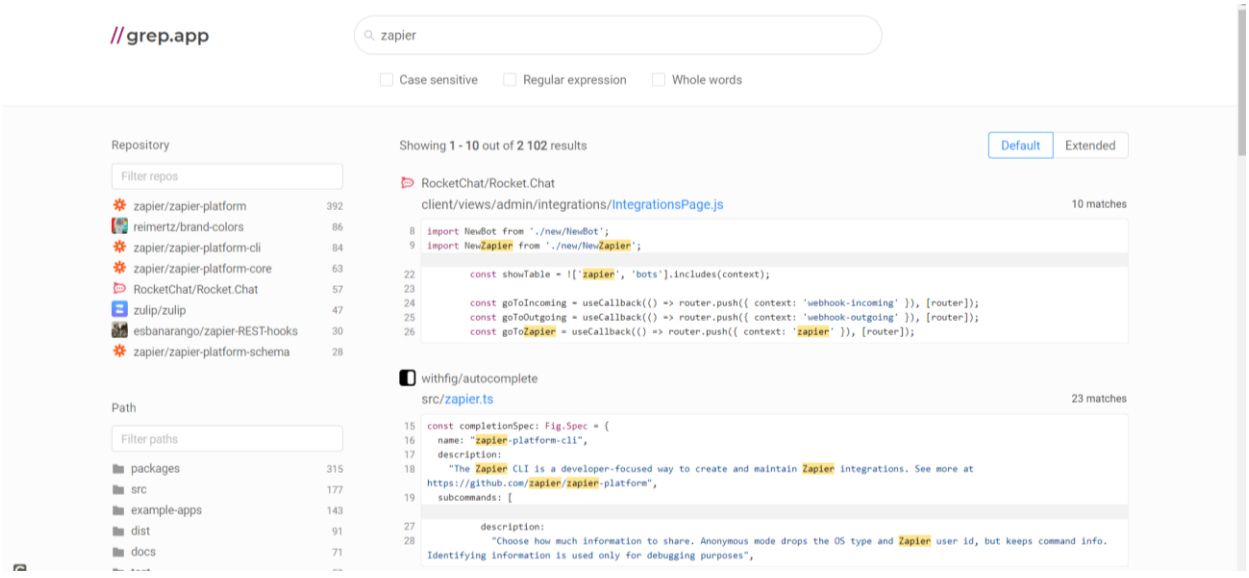
Базы данных Zapier не были слиты/опубликованы на RaidForums. Но большая часть сотрудников Zapier зарегистрирована на LinkedIn, чью БД можно найти на RaidForums, что в свою очередь дает возможность получить доступ к паролям и email.

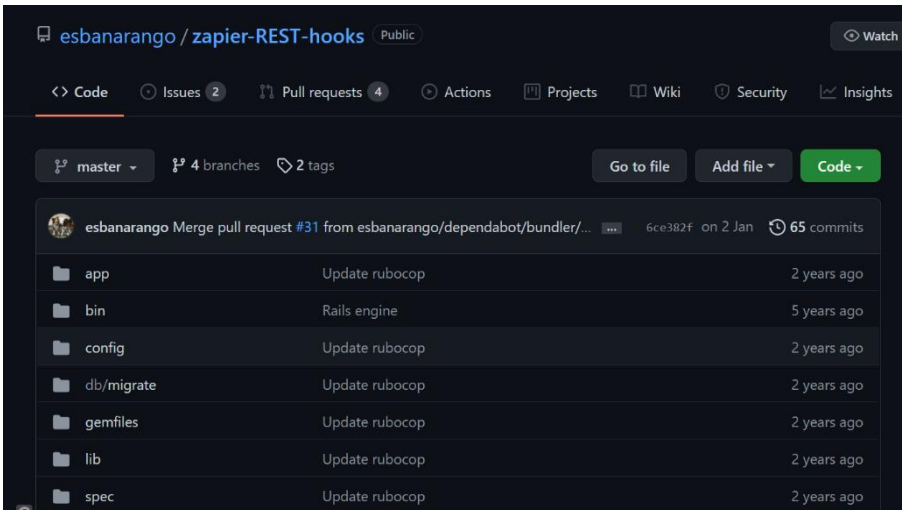




8. grep.app

По результатам исследования были найдены следующие различные репозитории с упоминанием Zapier, но какой-либо “интересной” информации найдено не было. Из полезного: найден github репозиторий с REST hooks (ручками). В описании говорится о том, что это hooks pattern. Нет во вкладке репозитории в профиле аккаунта компании Zapier.





Ссылка: https://github.com/esbanarango/zapier-REST-hooks

9. github.com/yogeshojha/rengin

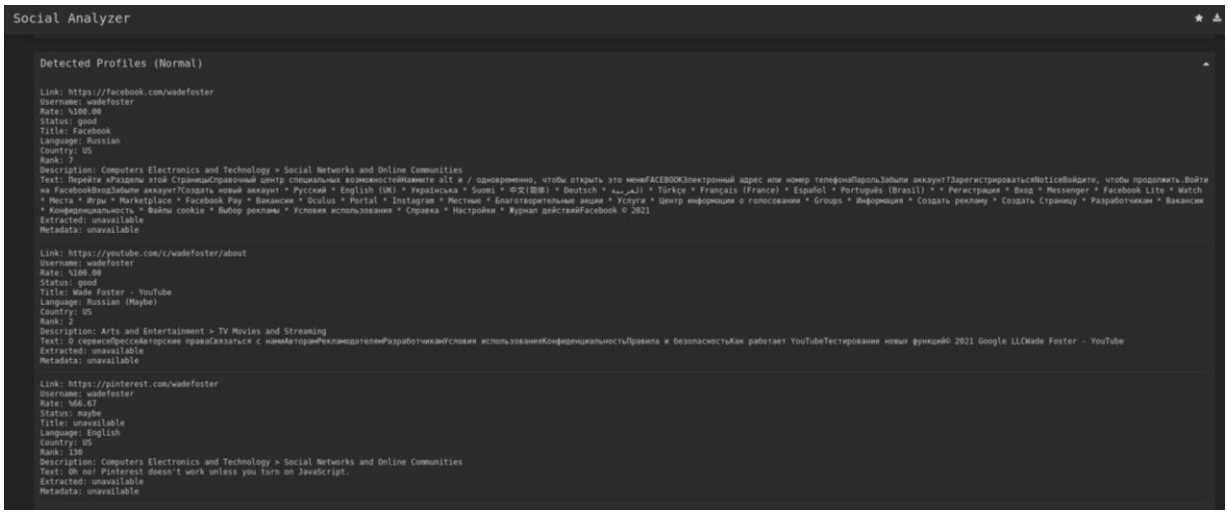
Были получены метаданные, в числе которых данные о различном ПО, API для просмотра, печати и управления PDF-файлами Adobe PDF library, графический движок Skia и тп. Весомого вклада в расследование не принесло.

10. github.com/qeeqbox/social-analyzer

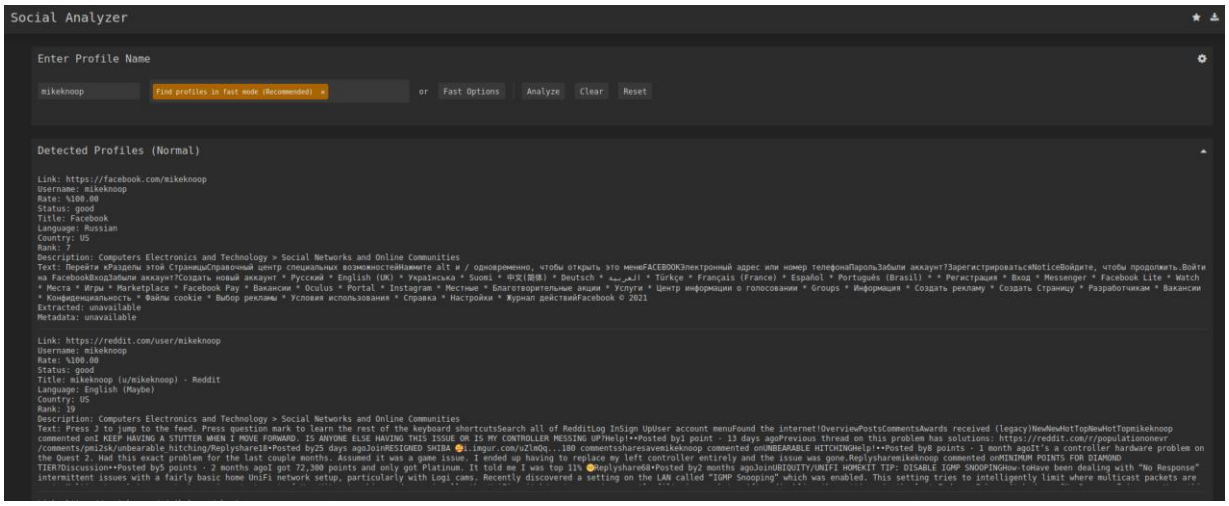
При помощи данного инструмента был произведен поиск аккаунтов соцсетей некоторых сотрудников Zapier. Ссылки, найденные на данном этапе указаны в разделе Данные о сотрудниках.

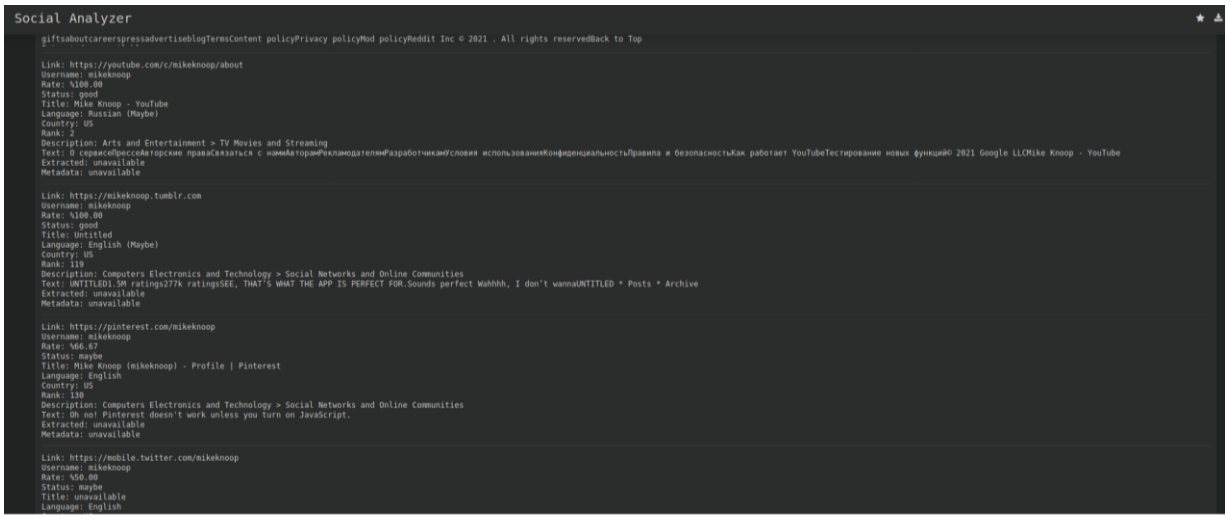
В числе которых:

Wade Foster (Co-founder & CEO)

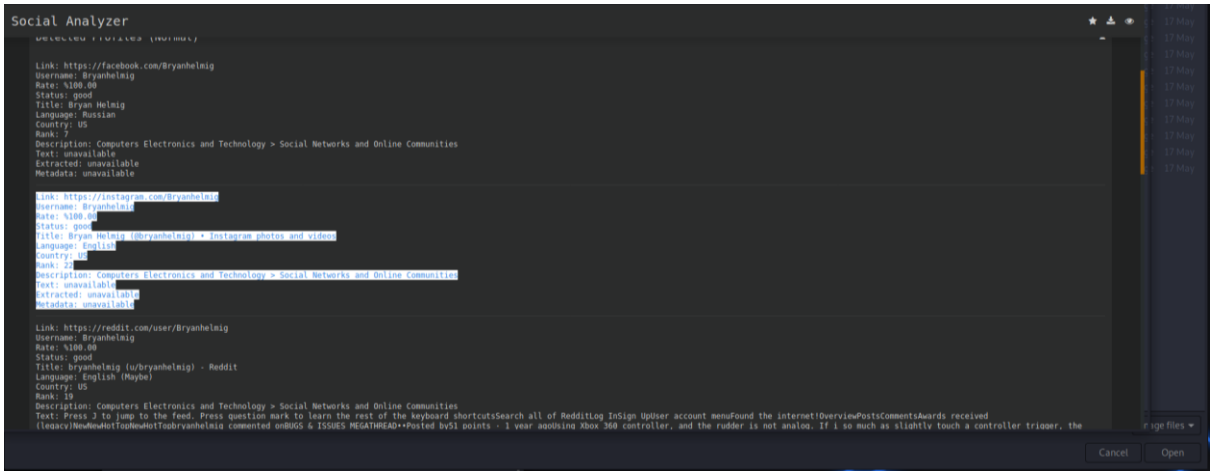


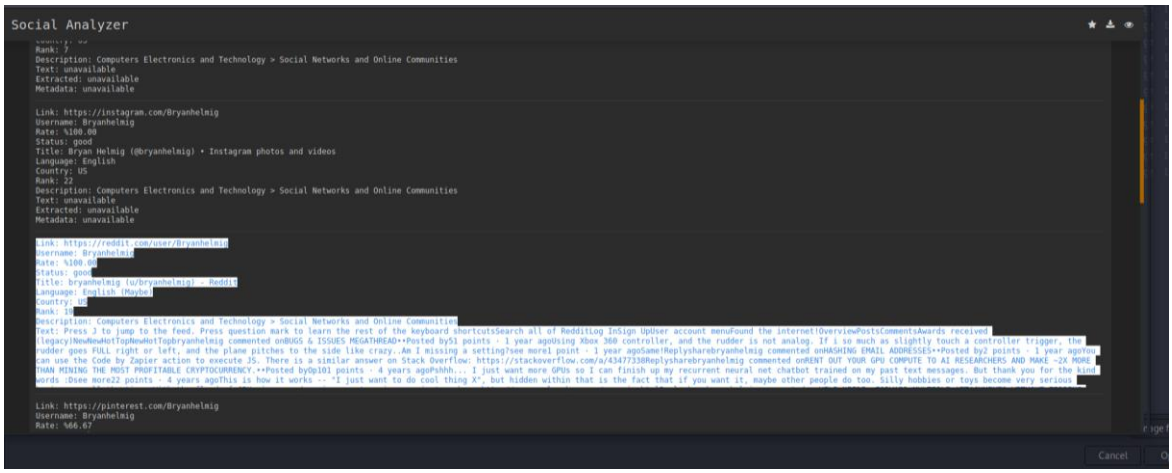
Mike Knoop (Co-founder, President)

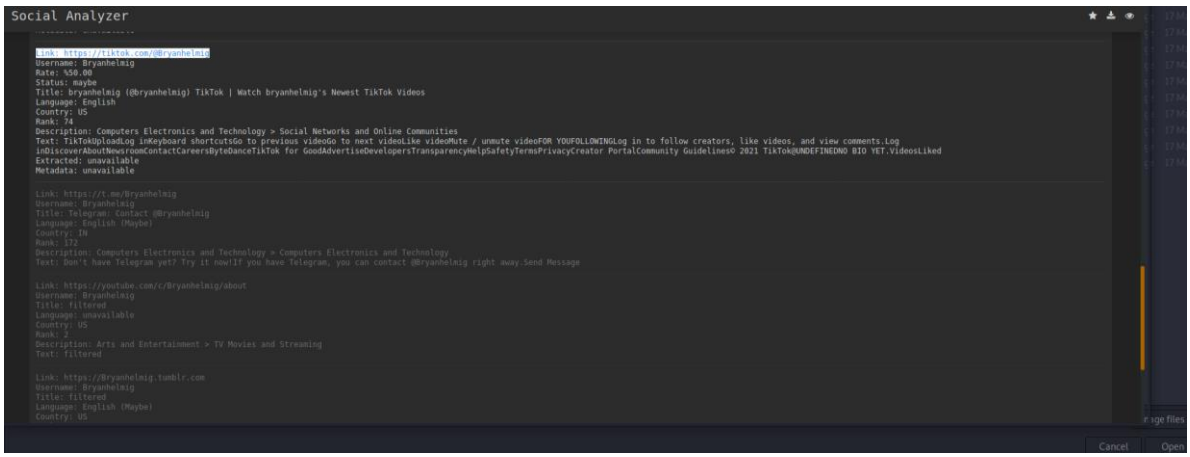


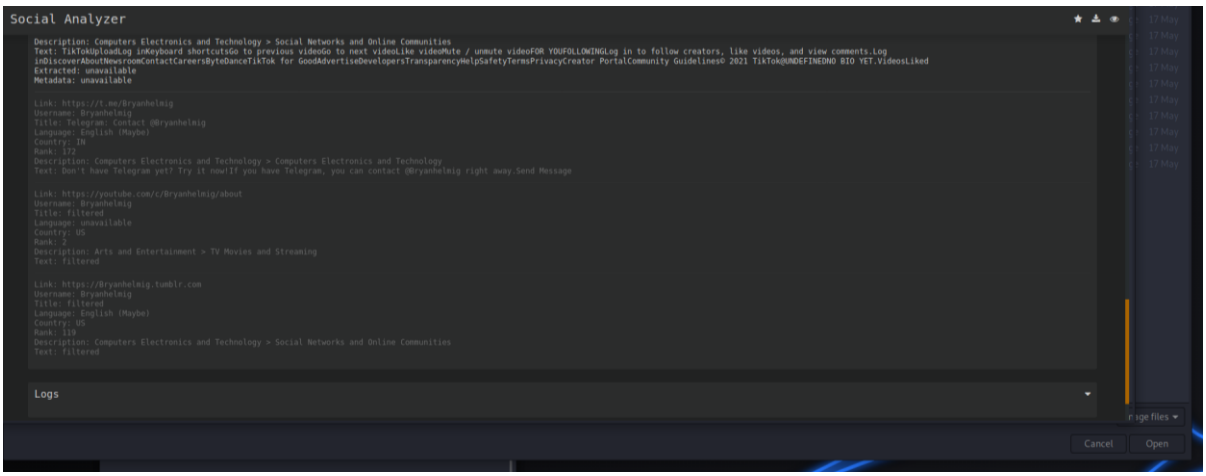


Bryan Helmig (Co-founder & CTO)

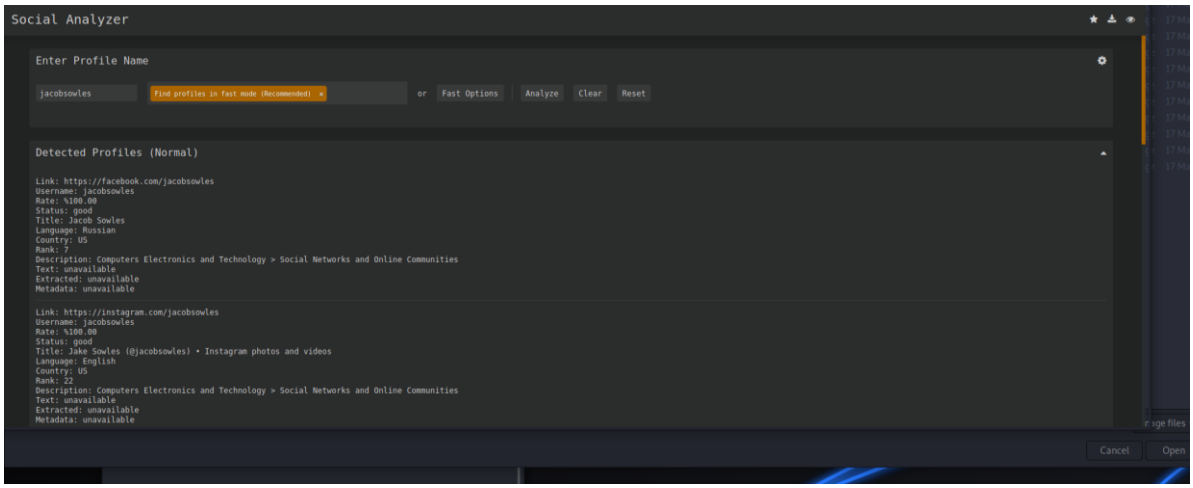




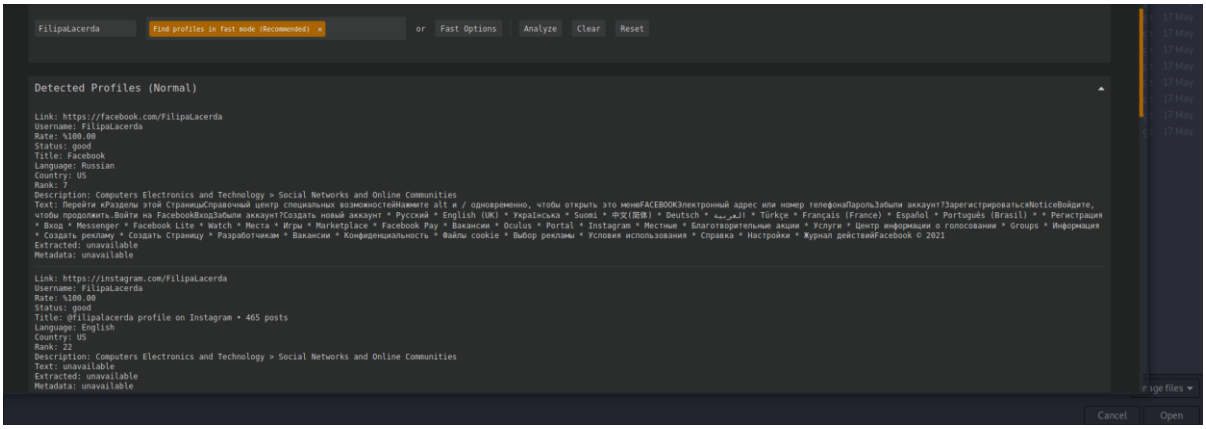




Jacob Sowels (Senior frontend)

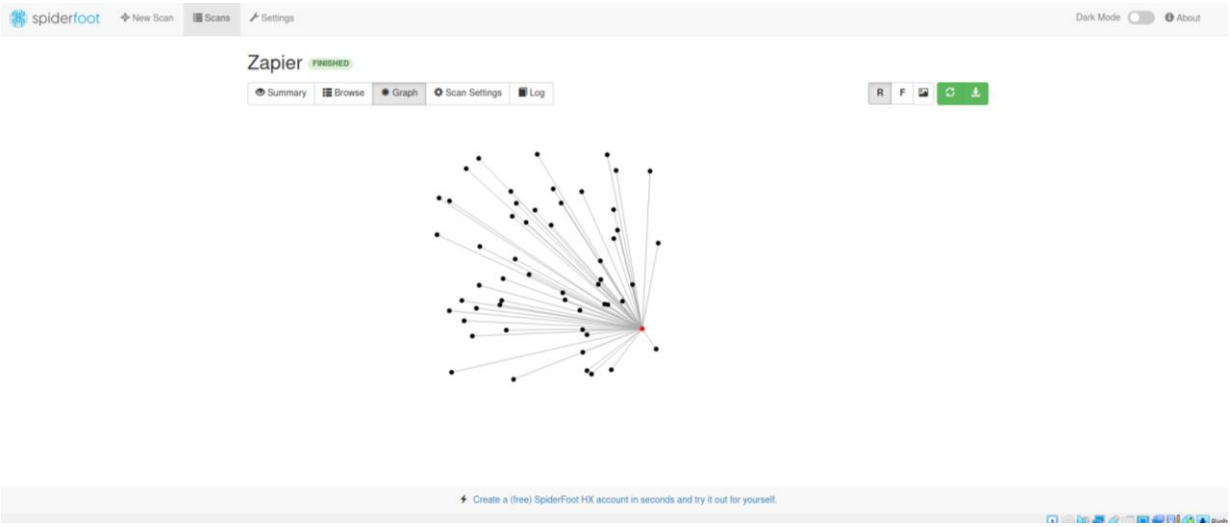


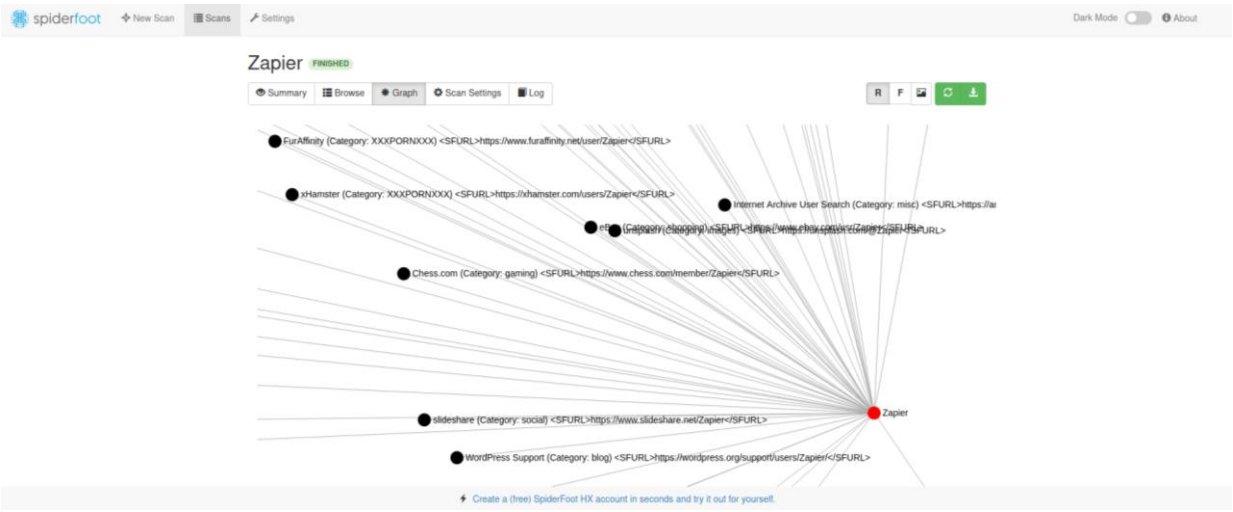
Filipa Lacerda (Senior frontend)



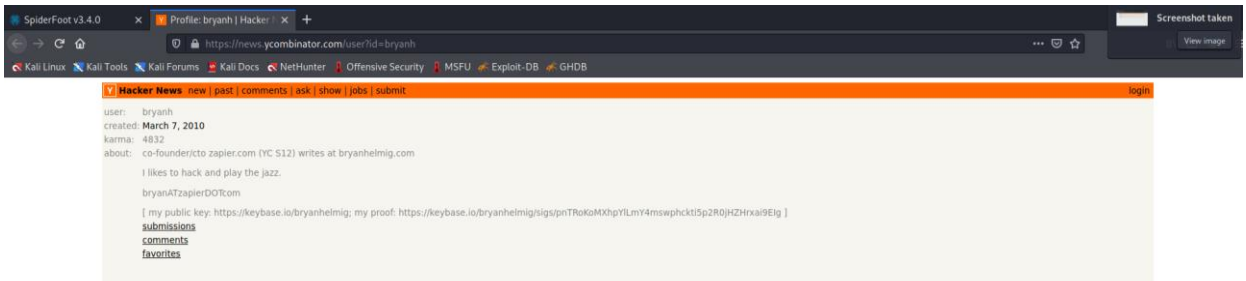
11. github.com/smicallef/spiderfoot

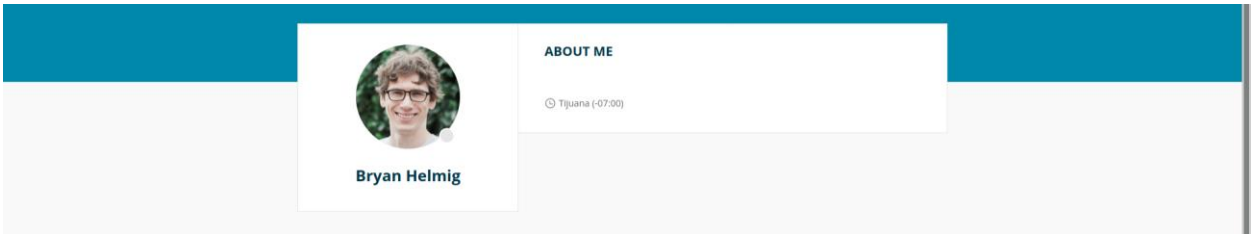
При использовании данного инструмента, был получен граф, построенный по информации, которая относится к Zapier.



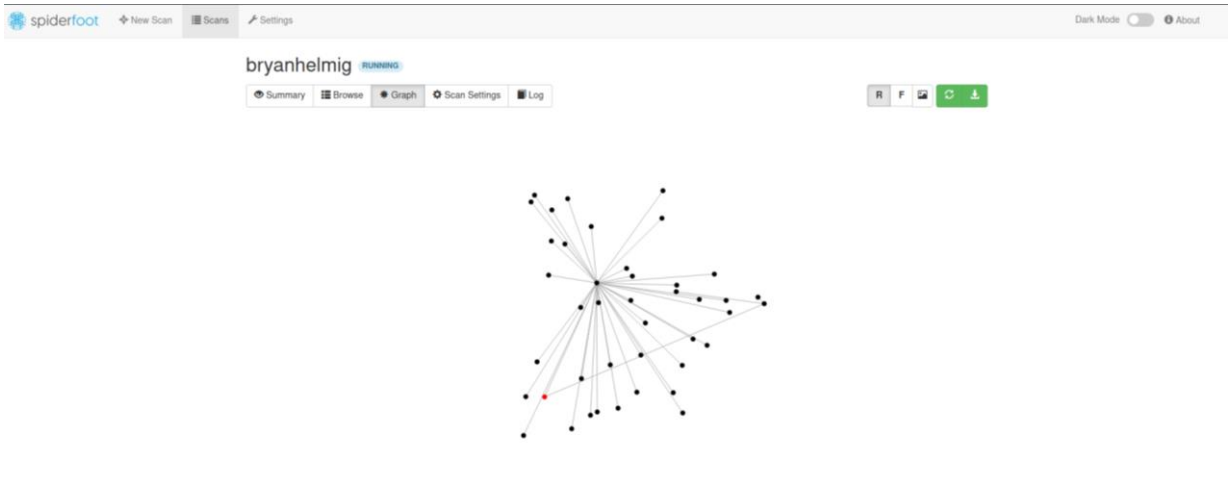


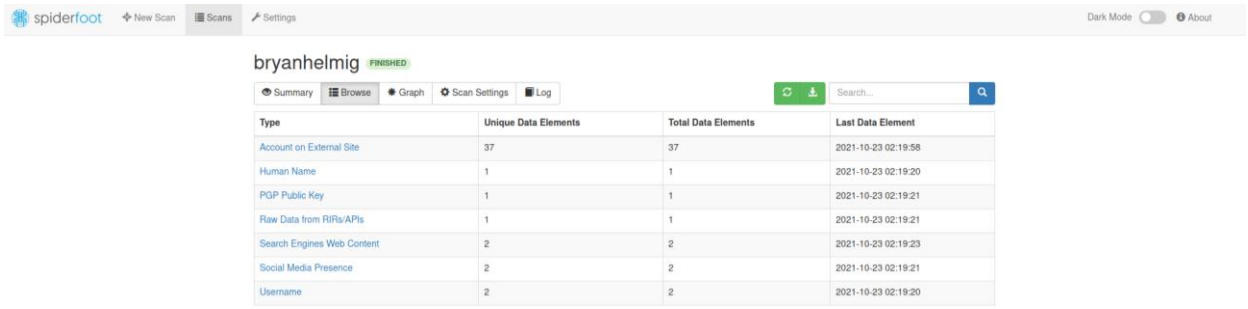
Также, данный инструмент позволил получить профиль Bryan Helmig на harcker news и codementor.

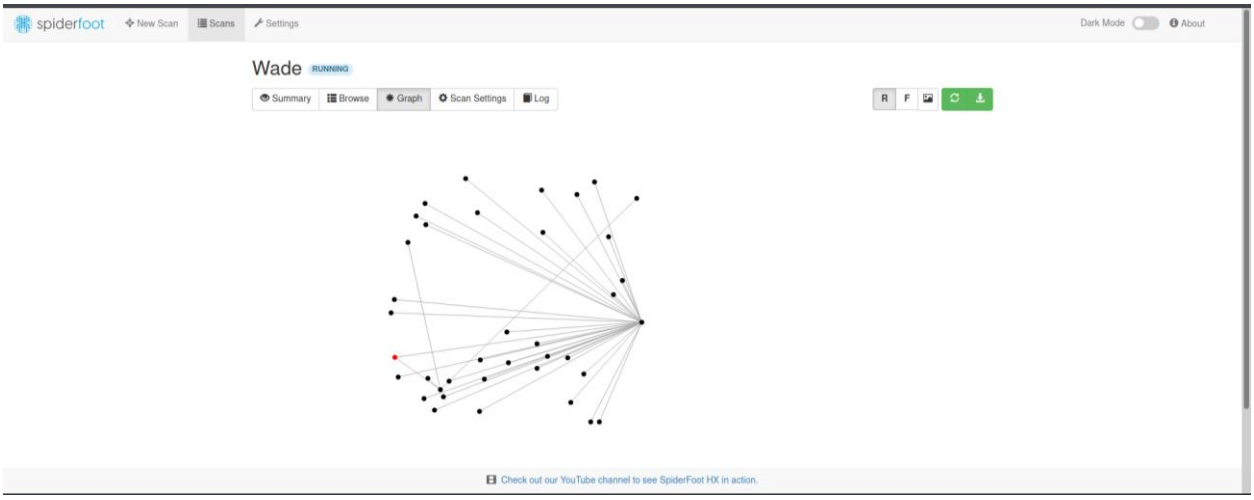




Указан предполагаемый часовой пояс.

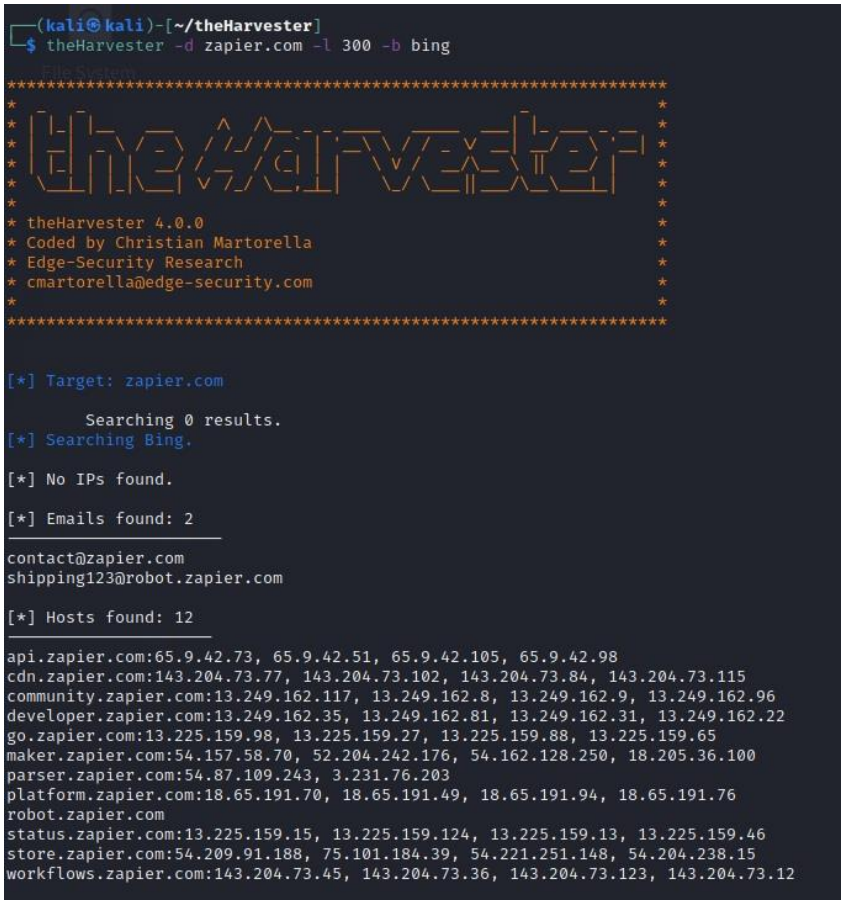






Граф Wade Foster. Какой-либо juicy информации найдено не было.

12. github.com/laramies/theHarvester



По результатам исследования были получены поддомены zapier.com. Дальнейшая разведка по данному пути не продолжалась.

13. github.com/zricethezav/gitleaks

По результатам сканирования основного репозитория с названием «zapier-platform» профиля Zapier на github, была обнаружена 1 утечка информации, что говорит о том, что где-то хранится пароль, API keys или токены.

На скрине ниже приведен кусок js кода, в котором gitleaks нашел утечку. По “const” и “fake”, а также по названию папки “test” (https://github.com/zapier/zapier-platform...zapier-platform-

core/test/tools/mocky.js), мы можем судить о том, что данная константа, скорее всего служит для проверки ошибок, тестирования, аутентификации или т.п. и не несет угрозы.

```
const fakeSignedPostData = {
  url: 'http://s3-fake.zapier.com/',
  fields: {
    policy: 'bm8gZHJhbWE=',
    AWSAccessKeyId: 'AKIAIKIAAKIAIKIAAKIA',
    acl: 'public-read',
    key: 'some-route/d362f087-1106-4847-9261-669ec340b580',
    signature: 'c4GzkaCtrc0ruvbZh6aSmf/1k='
  }
};
```

14. github.com/sherlock-project/sherlock

```
┌──(kali㉿kali)-[~/sherlock]
└─$ python3 sherlock BryanHelmig bryan-helmig bryan_helmig --timeout 30
[*] Checking username BryanHelmig on:
[+] Audiojungle: https://audiojungle.net/user/BryanHelmig
[+] Bandcamp: https://www.bandcamp.com/BryanHelmig
[+] BitBucket: https://bitbucket.org/BryanHelmig/
[+] Disqus: https://disqus.com/BryanHelmig
[+] Dribbble: https://dribbble.com/BryanHelmig
[+] Facebook: https://www.facebook.com/BryanHelmig
[+] Flipboard: https://flipboard.com/@BryanHelmig
[+] FortniteTracker: https://fortnitetracker.com/profile/all/BryanHelmig
[+] Freesound: https://freesound.org/people/BryanHelmig/
[+] GitHub: https://www.github.com/BryanHelmig
[+] GitLab: https://gitlab.com/BryanHelmig
[+] Gravatar: http://en.gravatar.com/BryanHelmig
[+] ICQ: https://icq.im/BryanHelmig
[+] IFTTT: https://www.ifttt.com/p/BryanHelmig
[+] Imgur: https://imgur.com/user/BryanHelmig
[+] Keybase: https://keybase.io/BryanHelmig
[+] Kik: https://kik.me/BryanHelmig
[+] LeetCode: https://leetcode.com/BryanHelmig
[+] Medium: https://medium.com/@BryanHelmig
[+] MixCloud: https://www.mixcloud.com/BryanHelmig/
[+] Pastebin: https://pastebin.com/u/BryanHelmig
[+] Periscope: https://www.periscope.tv/BryanHelmig/
[+] Pinterest: https://www.pinterest.com/BryanHelmig/
[+] ProductHunt: https://www.producthunt.com/@BryanHelmig
[+] PyPi: https://pypi.org/user/BryanHelmig
[+] Reddit: https://www.reddit.com/user/BryanHelmig
[+] Repl.it: https://repl.it/@BryanHelmig
[+] Slack: https://BryanHelmig.slack.com
[+] SlideShare: https://slideshare.net/BryanHelmig
[+] SoundCloud: https://soundcloud.com/BryanHelmig
[+] Spotify: https://open.spotify.com/user/BryanHelmig
[+] TikTok: https://tiktok.com/@BryanHelmig
[+] Trello: https://trello.com/BryanHelmig
[+] Twitch: https://www.twitch.tv/BryanHelmig
[+] Ultimate-Guitar: https://ultimate-guitar.com/u/BryanHelmig
[+] last.fm: https://last.fm/user/BryanHelmig

[*] Checking username bryan-helmig on:
[+] HackerNews: https://news.ycombinator.com/user?id=bryan-helmig
[+] Houzz: https://houzz.com/user/bryan-helmig
[+] ICQ: https://icq.im/bryan-helmig
[+] Pastebin: https://pastebin.com/u/bryan-helmig

[*] Checking username bryan_helmig on:
[+] Discuss.Elastic.co: https://discuss.elastic.co/u/bryan_helmig
[+] Disqus: https://disqus.com/bryan_helmig
[+] HackerNews: https://news.ycombinator.com/user?id=bryan_helmig
[+] Houzz: https://houzz.com/user/bryan_helmig
[+] ICQ: https://icq.im/bryan_helmig
```

```
┌──(kali㉿kali)-[~/sherlock]
└─$ python3 sherlock Zapier
[*] Checking username Zapier on:
[+] AskFM: https://ask.fm/Zapier
[+] Audiojungle: https://audiojungle.net/user/Zapier
```

```
┌──(kali㉿kali)-[~/sherlock]
└─$ python3 sherlock WadeFoster wade-foster c.wadefoster --timeout 30
[*] Checking username WadeFoster on:
[+] About.me: https://about.me/WadeFoster
[+] Blogger: https://WadeFoster.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/WadeFoster
[+] Contently: https://WadeFoster.contently.com/
[+] Disqus: https://disqus.com/WadeFoster
[+] Dribbble: https://dribbble.com/WadeFoster
[+] Duolingo: https://www.duolingo.com/profile/WadeFoster
[+] Facebook: https://www.facebook.com/WadeFoster
[+] Flickr: https://www.flickr.com/people/WadeFoster
[+] Flipboard: https://flipboard.com/@WadeFoster
[+] Freesound: https://freesound.org/people/WadeFoster/
[+] GitHub: https://www.github.com/WadeFoster
[+] Gravatar: http://en.gravatar.com/WadeFoster
[+] HackerNews: https://news.ycombinator.com/user?id=WadeFoster
[+] ICQ: https://icq.im/WadeFoster
[+] IFTTT: https://www.ifttt.com/p/WadeFoster
[+] Kik: https://kik.me/WadeFoster
[+] Medium: https://medium.com/@WadeFoster
[+] Myspace: https://myspace.com/WadeFoster
[+] Periscope: https://www.periscope.tv/WadeFoster/
[+] ProductHunt: https://www.producthunt.com/@WadeFoster
[+] Reddit: https://www.reddit.com/user/WadeFoster
[+] ReverbNation: https://www.reverbnation.com/WadeFoster
[+] Roblox: https://www.roblox.com/user.aspx?username=WadeFoster
[+] Slack: https://WadeFoster.slack.com
[+] SlideShare: https://slideshare.net/WadeFoster
[+] Smule: https://www.smule.com/WadeFoster
[+] Spotify: https://open.spotify.com/user/WadeFoster
[+] TikTok: https://tiktok.com/@WadeFoster
[+] Trello: https://trello.com/WadeFoster
[+] Twitch: https://www.twitch.tv/WadeFoster
[+] Wattpad: https://www.wattpad.com/user/WadeFoster
[+] Xbox Gamertag: https://xboxgamertag.com/search/WadeFoster

[*] Checking username wade-foster on:
[+] HackerNews: https://news.ycombinator.com/user?id=wade-foster
[+] Houzz: https://houzz.com/user/wade-foster
[+] ICQ: https://icq.im/wade-foster
[+] MixCloud: https://www.mixcloud.com/wade-foster/
[+] SoundCloud: https://soundcloud.com/wade-foster
[+] Xbox Gamertag: https://xboxgamertag.com/search/wade-foster

[*] Checking username c.wadefoster on:
[+] EyeEm: https://www.eyeem.com/u/c.wadefoster
[+] Facebook: https://www.facebook.com/c.wadefoster
[+] HackerNews: https://news.ycombinator.com/user?id=c.wadefoster
[+] HackerRank: https://hackerrank.com/c.wadefoster
[+] ICQ: https://icq.im/c.wadefoster
[+] Splits.io: https://splits.io/users/c.wadefoster
```

```
┌──(kali㉿kali)-[~/sherlock]
└─$ python3 sherlock ibolmo
[*] Checking username ibolmo on:
[+] Apple Discussions: https://discussions.apple.com/profile/ibolmo
[+] Audiojungle: https://audiojungle.net/user/ibolmo
[+] Blogger: https://ibolmo.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/ibolmo
```

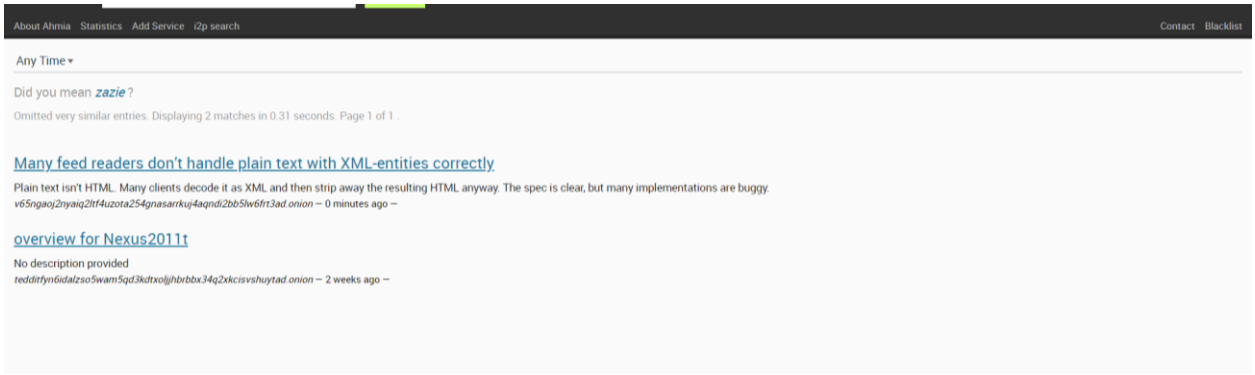
При помощи сервиса Sherlock были найдены различные соцсети некоторых сотрудников компании. Однако, большая часть полученных ссылок либо ведет на удаленные страницы, либо относится к другим людям, не имеющим отношения к компании Zapier.

15. github.com/s0md3v/Photon

```
┌──(kali㉿kali)-[~/Photon]
└─$ python3 photon.py -u zapier.com                                  127 ×
                    ___ _           _
                   / _ \ |__   ___ | |_ ___  _ __
                  / /_)/ '_ \ / _ \| __/ _ \| '_ \
                 / ___/| | | | (_) | || (_) | | | |
                 \/    |_| |_|\___/ \__\___/|_| |_|
                                                v1.3.2
[+] URLs retrieved from robots.txt: 19
[+] URLs retrieved from sitemap.xml: 29
[~] Level 1: 46 URLs
```

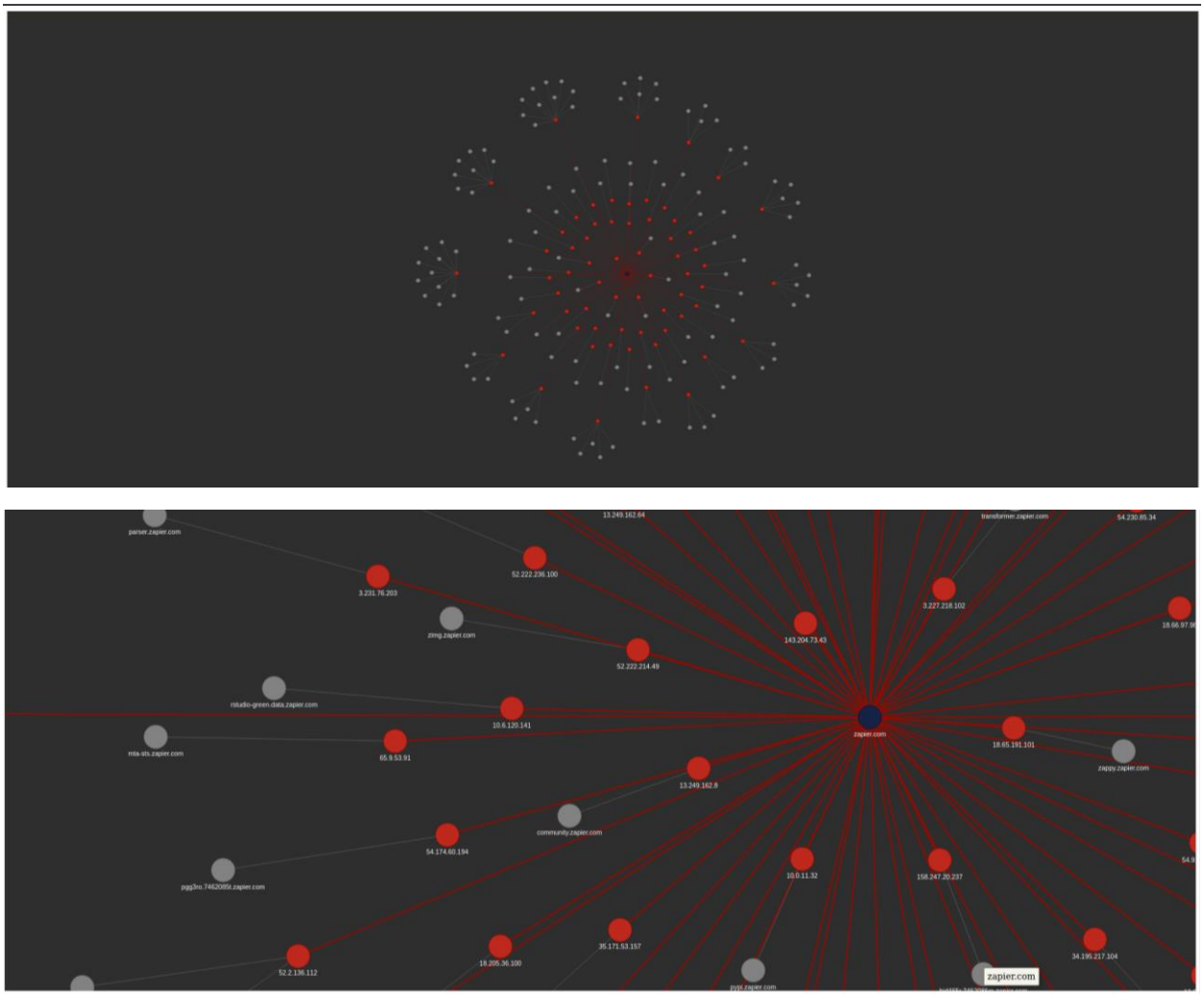
Информация (именно – поддомены компании), предоставленная данным сервисом, едва ли может считаться полезной, поскольку схожие ведения уже были предоставлены иными средствами.

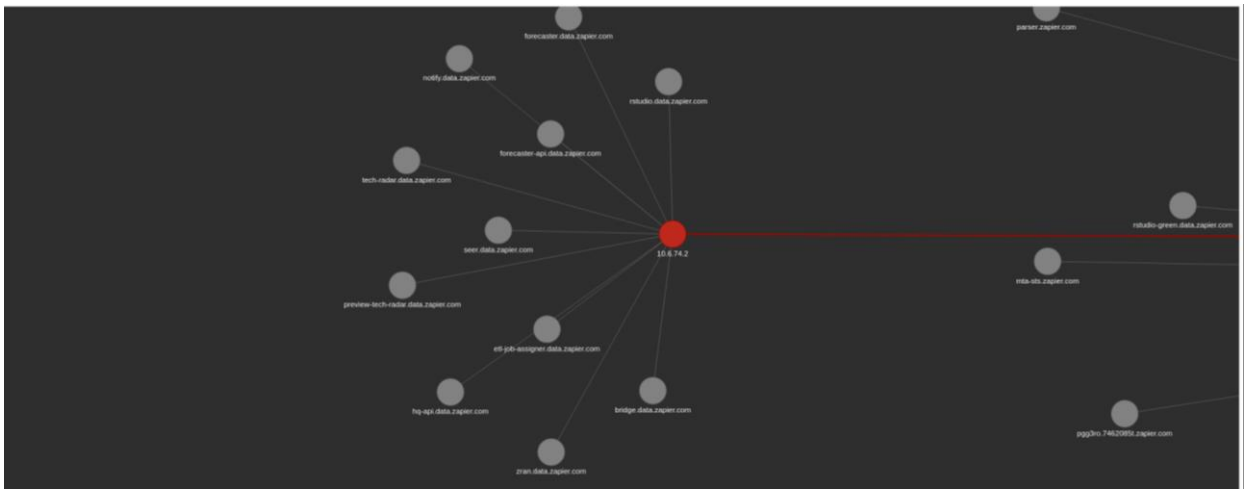
16. ahmia.fi

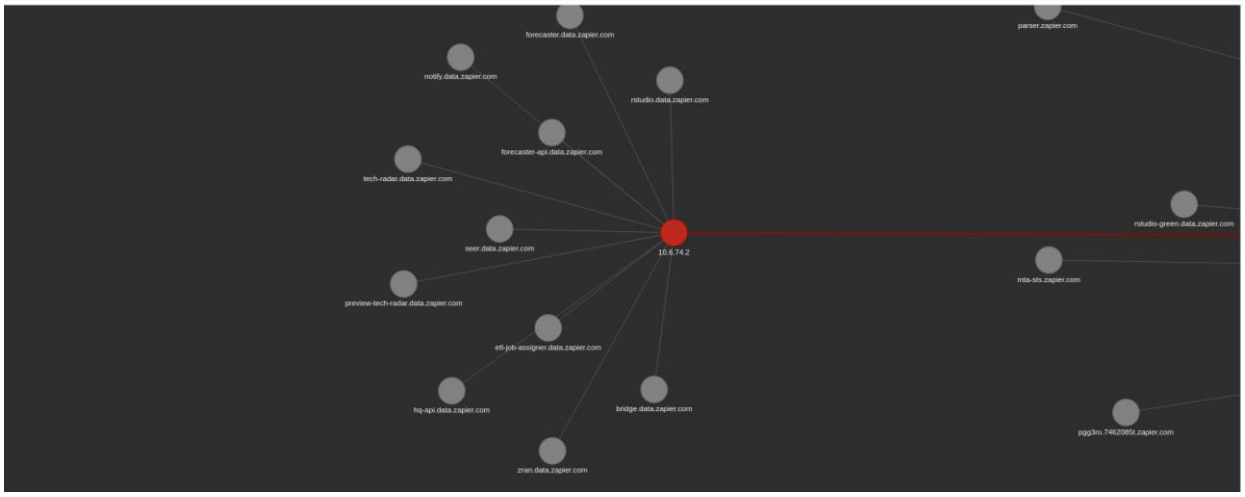


Поиск по запросу «Zapier» на данной платформе не дал результатов – две ссылки на блоги/статьи неизвестных людей, в которых Zapier упоминается в качестве примера ПО.

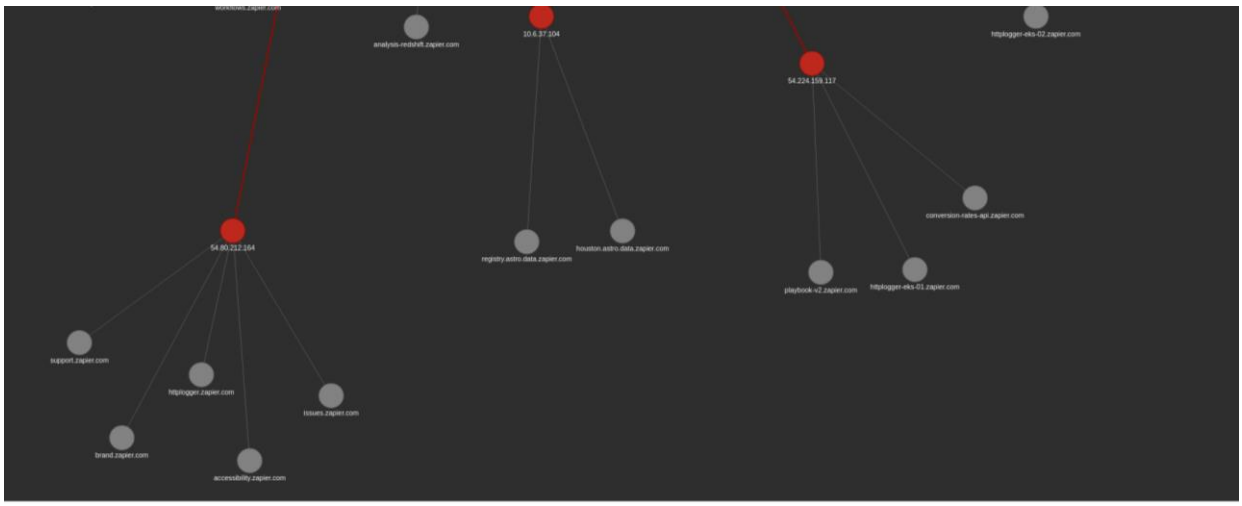
17. github.com/screetsec/Sudomy

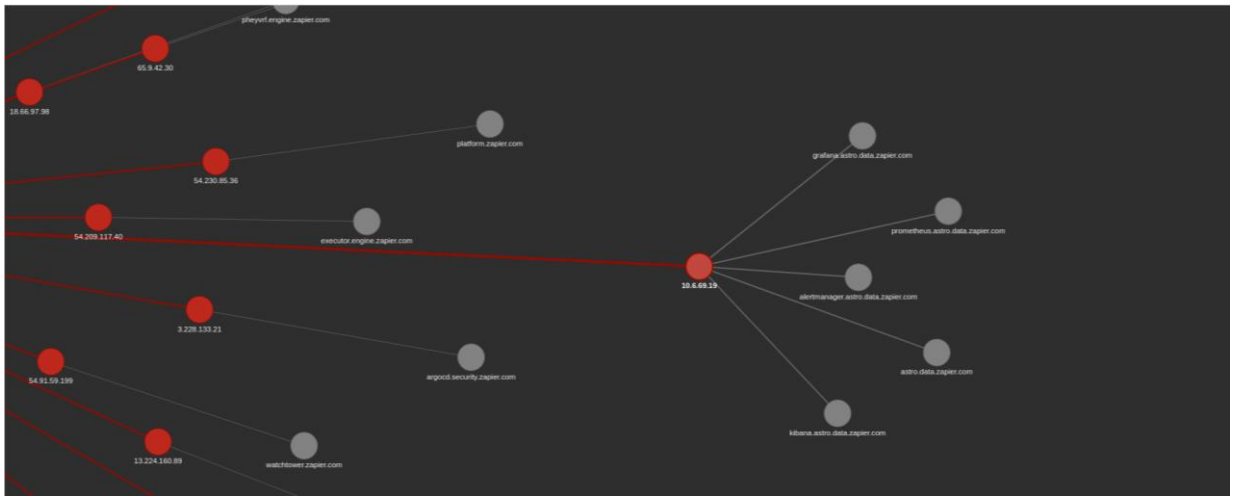



forecaster.data.zapier.com
parser.zapier.com
notify.data.zapier.com
rstudio.data.zapier.com
forecaster-api.data.zapier.com
tech-radar.data.zapier.com
rstudio-green.data.zapier.com
seer.data.zapier.com
10.6.74.2
mta-sts.zapier.com
preview-tech-radar.data.zapier.com
ml-job-assigner.data.zapier.com
hq-api.data.zapier.com
bridge.data.zapier.com
pgg3ro.74620851.zapier.com
zran.data.zapier.com


forecaster.data.zapier.com
parser.zapier.com
notify.data.zapier.com
rstudio.data.zapier.com
forecaster-api.data.zapier.com
tech-radar.data.zapier.com
rstudio-green.data.zapier.com
seer.data.zapier.com
10.6.74.2
mta-sts.zapier.com
preview-tech-radar.data.zapier.com
ml-job-assigner.data.zapier.com
hq-api.data.zapier.com
bridge.data.zapier.com
pgg3ro.74620851.zapier.com
zran.data.zapier.com


retreat.zapier.com
swb-image-service.zapier.com
incident-playbook.zapier.com
mapier-api.zapier.com
design.zapier.com
msteams.zapier.com
async.zapier.com
contentfulwebhook.zapier.com
support-api.zapier.com
34.200.138.115
mapier.zapier.com
api.tables.zapier.com
support-ops-es.zapier.com
tables.zapier.com
carvada-playbook.zapier.com
prometheus.zapier.com
explore-styleguide.zapier.com
23.23.168.39

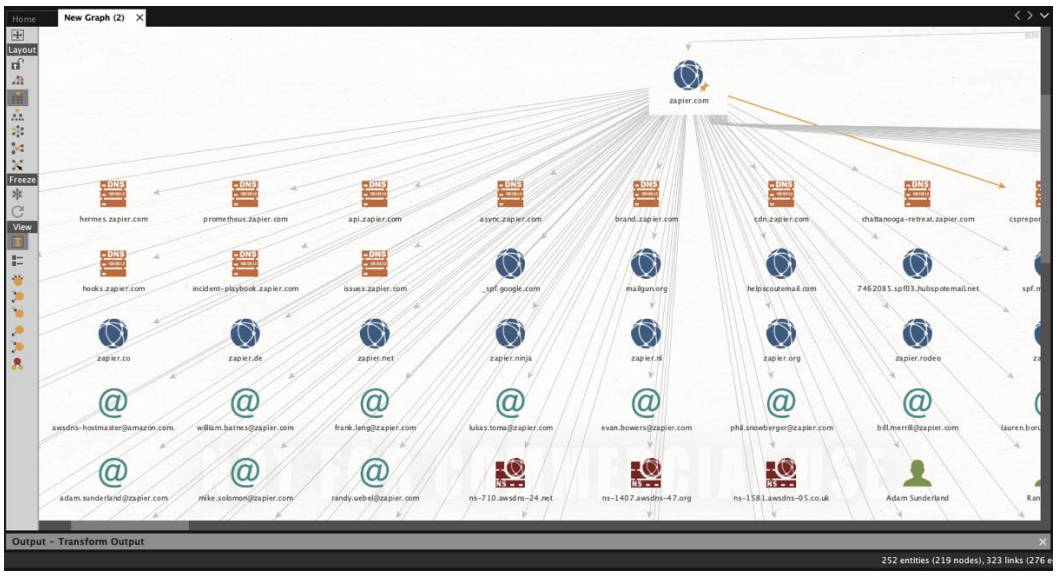




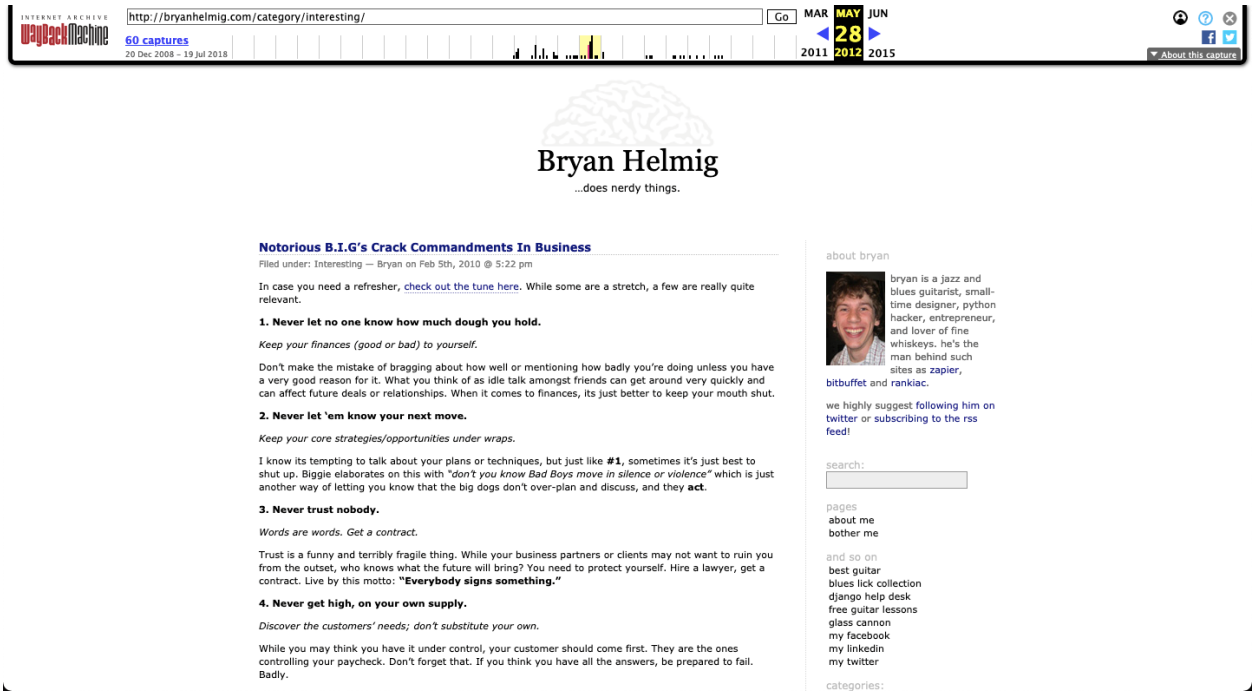
По результатам исследования были получены имена поддоменов Zapier.

18. Maltego

При помощи данного средства был осуществлен поиск как по доменному имени самой компании, так и по электронной почте некоторых сотрудников. Сервис также позволил выявить полезную информацию: ip-адреса, связанные с компанией люди, номера телефонов. Однако, точность не всей информации из представленной удалось подтвердить при помощи иных сервисов.



При проверке электронной почты одного из сотрудников удалось найти ссылки с web.archive.org, однако сохраненные сервисом страницы содержат только личный блог, принадлежавший Bryan Helmig, который не несет особо полезной информации и сведений контактах сотрудника.



Данные о сотрудниках компании

Основные критерии:

1. Аккаунт на GitHub
2. Аккаунт на LinkedIn

3. Активное присутствие в соц. сетях (свежие посты и пр.)
4. Занимаемая должность – CEO, CTO, Senior Developer и т. д.

По итогам поиска информации решено было остановиться на 6 людях, которые занимают достаточно высокую должность в компании Zapier.

Bryan Helmig (Co-founder & CTO)

https://github.com/bryanhelmig

https://www.linkedin.com/in/bryanhelmig

https://www.facebook.com/bryanhelmig

https://twitter.com/bryanhelmig

bryan@zapier.com – корпоративная почта

bryan@bryanhelmig.com – личная почта

bryanhelmig@gmail.com – личная почта

@bryanhelmig – instagram

Wade Foster (Co-founder & CEO)

https://github.com/WadeFoster

https://www.linkedin.com/in/wadefoster/

https://www.facebook.com/c.wade.foster

https://twitter.com/wadefoster

c.wade.foster@gmail.com – личная почта

@cwadefoster – Instagram (закрытый аккаунт)

Mike Knoop (Co-founder, President)

https://github.com/mikeknoop

https://www.linkedin.com/in/mikeknoop/

https://twitter.com/mikeknoop

https://mikeknoop.com – личный сайт

mike@zapier.com – корпоративная почта

mikeknoop@gmail.com – личная почта

@mikeknoop – instagram

Olmo Maldonado (Sr. Engineer, Backend)

https://github.com/ibolmo

https://www.linkedin.com/in/olmom/

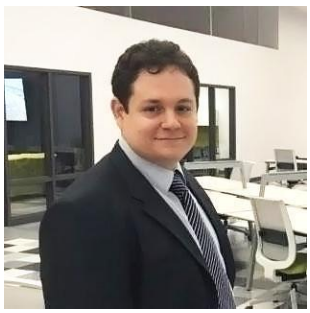
https://www.facebook.com/ibolmo

https://twitter.com/ibolmo

http://ibolmo.com – личный сайт

me@ibolmo.com – личная почта

@ibolmo – instagram (закрытый аккаунт)



Jacob Sowles (Sr. Engineer, Frontend)

https://github.com/jacobsowles

https://www.linkedin.com/in/jacobsowles/

jrsowles@gmail.com – личная почта

Filipa Lacerda (Sr. Engineer, Frontend)

https://github.com/filipalacerda

https://www.linkedin.com/in/filipalacerda/

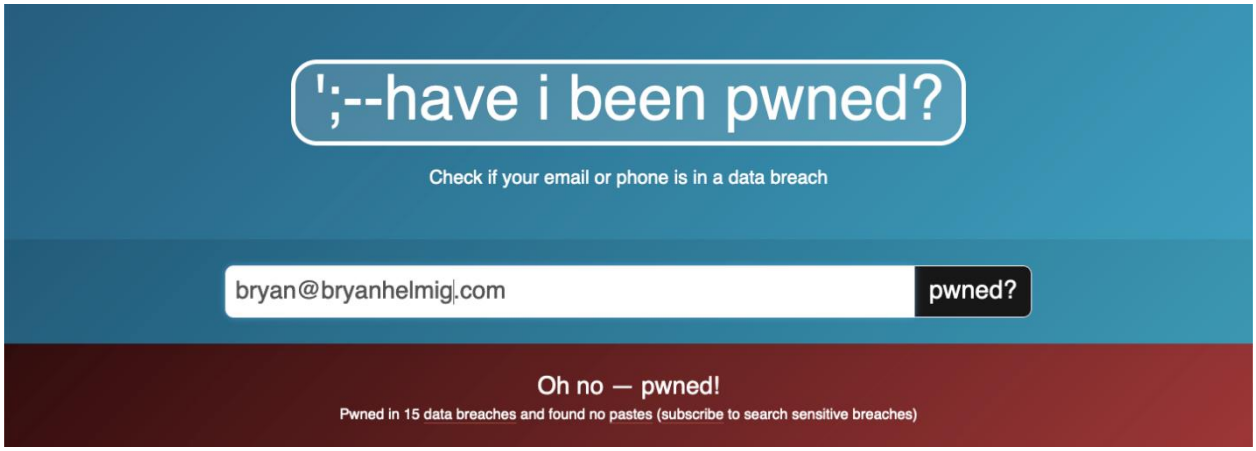
https://twitter.com/FilipaLacerda

lacerda.filipa@gmail.com – личная почта

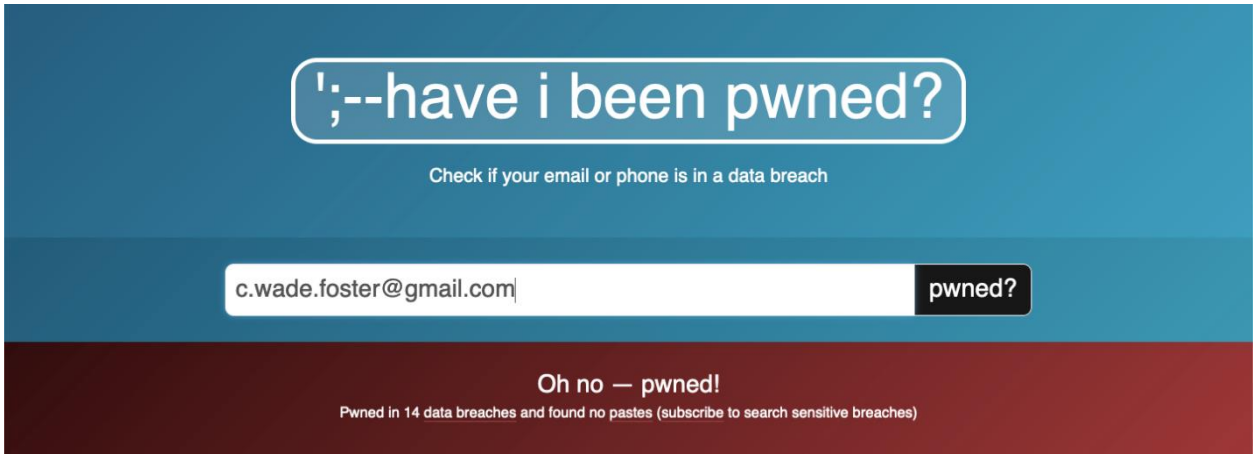
Изучение потенциальных жертв фишинговой атаки

Гарантировать успех фишинговой атаки на одного конкретного человека сложно, поэтому было принято решение о сборе информации по каждому из представленных выше сотруднику Zapier.

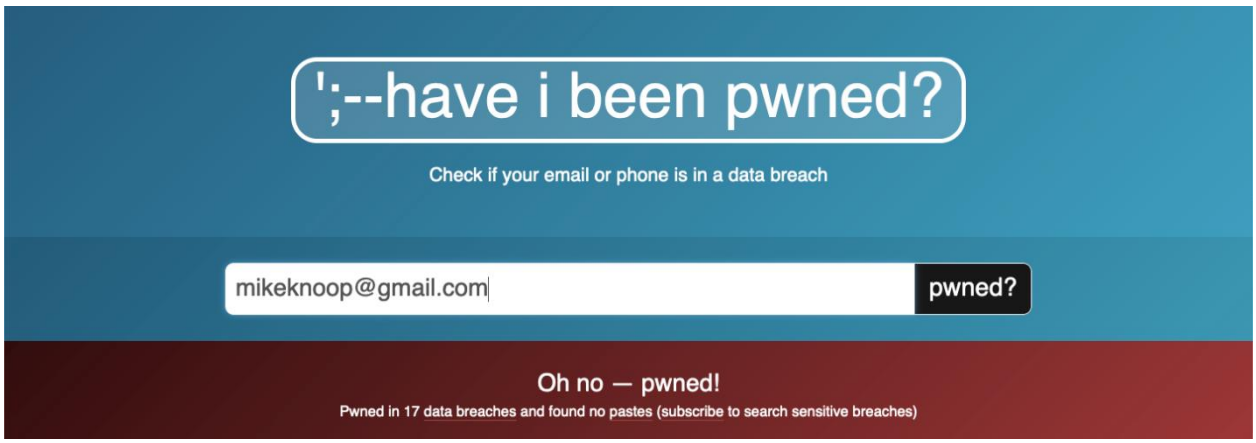
В связи с тем, что почта каждого из 6 описанных сотрудников нам известна, были проверены возможные утечки этих адресов с помощью сервиса https://haveibeenpwned.com/.



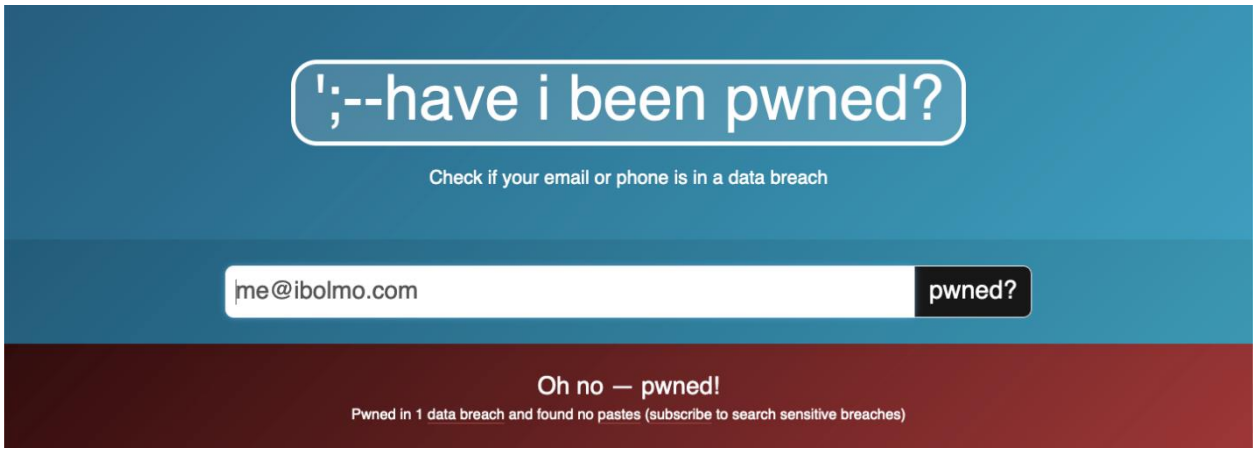
Личная почта, принадлежащая Bryan Helmig



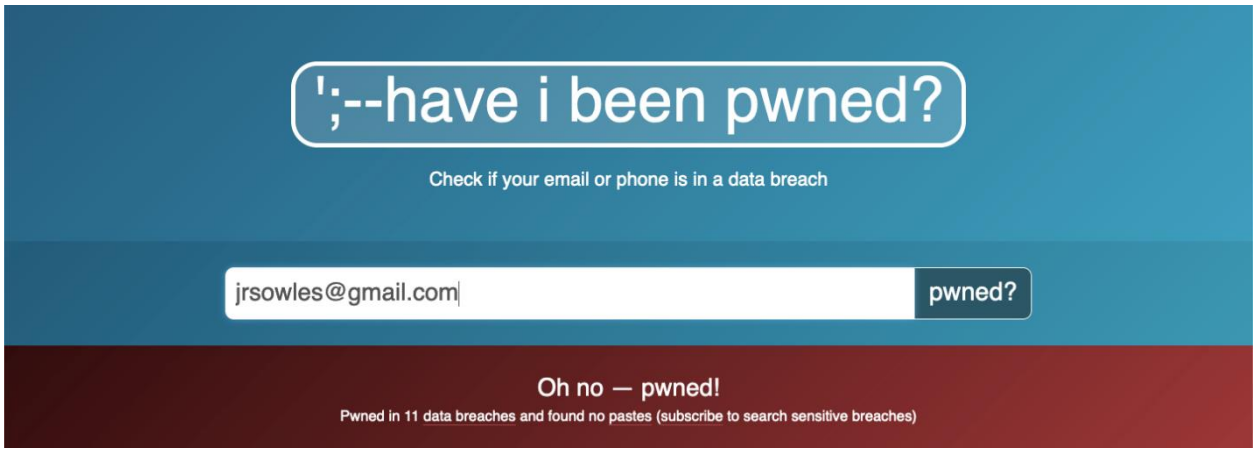
Личная почта, принадлежащая Wade Foster



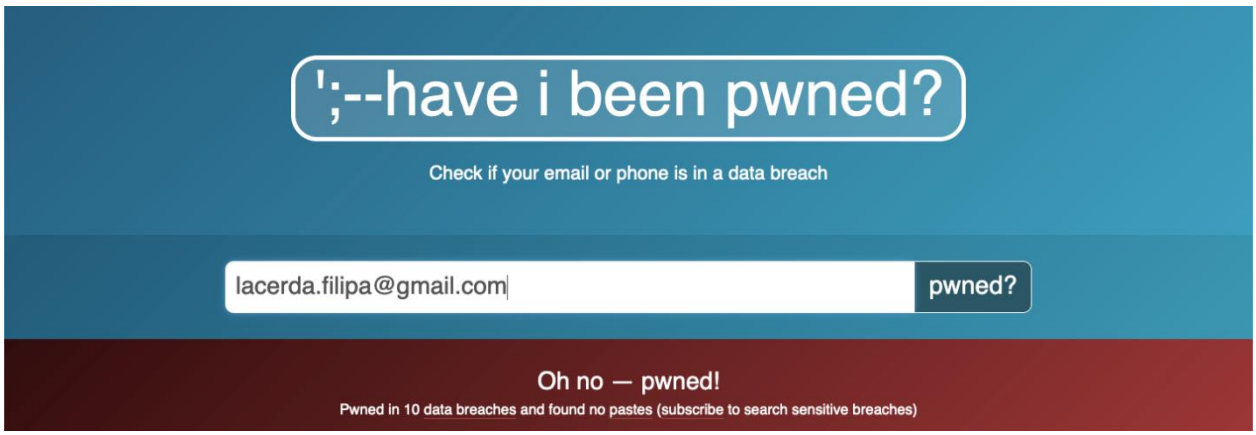
Личная почта, принадлежащая Mike Knoop



Личная почта, принадлежащая Olmo Maldonado



Личная почта, принадлежащая Jacob Sowles



Личная почта, принадлежащая Filipa Lacerda

Проверка показала, что все личные почты сотрудников были обнаружены в сливах, в связи с этим покупка слитых баз данных может предоставить как доступ к почте человека для дальнейшей атаки на Zapier, так и некоторую информацию для проведения фишинговой атаки.

Поскольку 2 из 6 сотрудников имеют собственные домены для личной почты (@bryanhelmig.com и @ibolmo.com), была произведена проверка данных доменов на https://whois.domaintools.com/, однако поиск не дал результатов, так как имена владельцев доменов оказались скрыты. Однако данные адреса были взяты с личных страниц этих сотрудников в соцсетях.

Поскольку выбранные нами сотрудники активно используют соцсети, было решено найти реальных людей, членов семьи и друзей, с которыми человек взаимодействует.

В качестве таких соцсетей были взяты Facebook и Instagram. Twitter сотрудников в основном используется для освещения корпоративных новостей о работе Zapier, поэтому для выяснения контактов людей он не подходит.

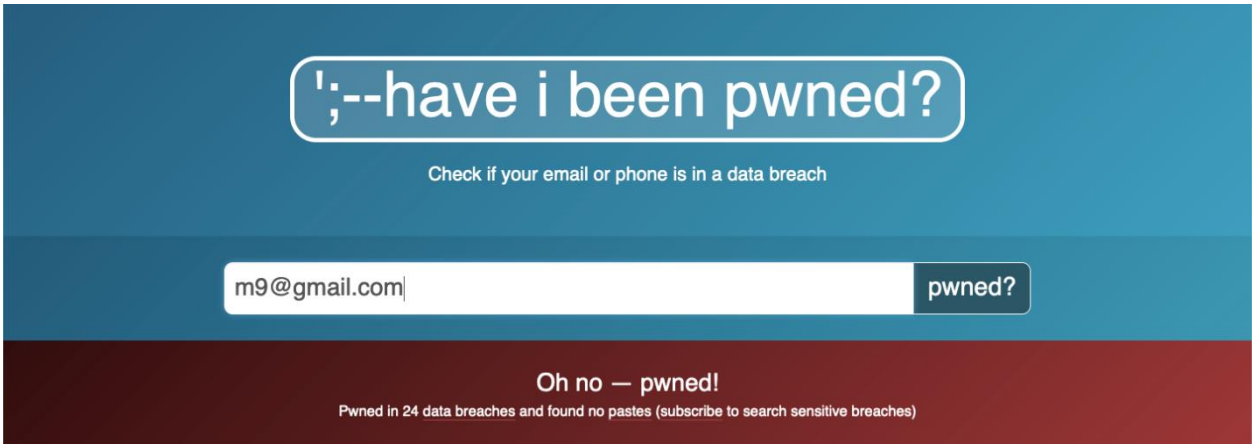
На личной странице Bryan Helmig в Facebook присутствуют ссылки на его сестру – Shelley Marie Helmig (https://www.facebook.com/shelley.helmig), а также на мать – Cheryl Helmig (https://www.facebook.com/cheryl.helmig).

Также несмотря на то, что Bryan Helmig не ведет свой Instagram-аккаунт достаточно активно (последняя публикация сделана в 2012 году), на его странице можно найти отметки на фото, сделанные его сестрой (@shelleyhelmig).

Судя по страницам Shelley Helmig в Facebook и Instagram, она проживает в г. Манхэттен, Нью-Йорк, т.е. в разных городах с Bryan Helmig (который живет в г. Сент-Луис, Миссури). Исходя из этого вполне можно использовать имя Shelley для совершения атаки.

К сожаленью, Amy Helmig, жена Bryan Helmig, работает в Mountain View Public Library на должности, которая не указана на официальном сайте библиотеки, что в некотором роде исключает её общение с большим количество людей посредством электронной почты. Поэтому дальнейший поиск информации о ней, с целью нахождения почты и получения доступа к семейному компьютеру Helmig не имеет смысла.

Что касается другого сотрудника, Mike Knoop, – личный профиль его жены, Michelle Knoop (@michellewknoop), был найден через функцию отметок на фото в Instagram. Через попытку сброса пароля была найдена её личная почта – m9@gmail.com, которая оказалась слита. Таким образом, через покупку баз данных вполне можно получить доступ к домашнему компьютеру Mike и Michelle Knoop.



Личная почта, принадлежащая Michelle Knoop

В следствие анализа личной страницы Olmo Maldonado на Facebook было выяснено, что его дочь владеет страницей магазина на

платформе Etsy (https://www.etsy.com/shop/KittyKissCo). Через связь с ней также вполне можно попытаться получить доступ к личному домашнему компьютеру семьи Maldonado.

Заключение

После проведенного анализа можно сделать вывод о том, что сотрудники, занимающие высокие должности в компании Zapier, ведут достаточно конфиденциальные профили в социальных сетях и особо не делятся личной информацией. Наибольший интерес для нас могут представлять Bryan Helmig и Mike Knoop, поскольку через них достаточно легко найти профили членов их семей, и далее от их лица осуществлять фишинговую атаку.

Однако стоит отметить, что сотрудники, информация о которых приведена в данном отчете, были выбраны случайным образом, поэтому поиск информации о других сотрудниках компании Zapier мог принести дополнительные сведения [2].

Поскольку личные почты всех 6 перечисленных выше сотрудников были обнаружены в нескольких слитых базах данных, получение доступа к этим сливам может предоставить пароли, а также иную чрезвычайно важную информацию об этих людях, которую можно использовать в дальнейшем. Но, к сожалению, без наличия этой личной информации данных для проведения атаки недостаточно.

Ссылки

1. https://en.wikipedia.org/wiki/Zapier
2. https://zapier.com/about/
3. https://zapier.com/