

## **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

The screenshot shows the Exploit Database interface. On the left is a vertical orange sidebar with icons for various tools. The main area has a dark header with the 'EXPLOIT DATABASE' logo. Below the header is a search bar with 'Search: zapier' and a 'Reset All' button. There are also 'Filters' and 'Show 15' buttons. The search results table has columns for 'Type', 'Platform', and 'Author'. A message at the top right says 'No matching records found'. At the bottom of the table, it says 'Showing 0 to 0 of 0 entries (filtered from 44,383 total entries)' and includes links for 'FIRST', 'PREVIOUS', 'NEXT', and 'LAST'.

Type	Platform	Author
Penetration Testing with Kali Linux (PWK) (PEN-200)	All new for 2020	Penetration Testing
Offensive Security Wireless Attacks (WiFu) (PEN-210)		Advanced Attack Simulation
Evasion Techniques and Breaching Defences (PEN-300)	All new for 2020	Application Security Assessment
Advanced Web Attacks and Exploitation (AWAE) (WEB-300)	Updated for 2020	
Windows User Mode Exploit Development (EXP-301)		

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

The screenshot shows the FOCA tool interface. At the top, it says 'Project of https://zapier.com/ - FOCA Open Source 3.4.7.1'. The menu includes 'Project', 'Plugins', 'Options', 'TaskList', 'About', and a shopping cart icon. The left pane is a tree view of the project structure under 'Project of https://zapier.com/'. It includes sections for 'Network', 'Domains', 'Document Analysis', and 'Metadata Summary'. Under 'Metadata Summary', there is a 'Users' section with 0 items. The right pane shows a table with 'Attribute' and 'Value' columns. It says 'All users found (0) - Times found' and 'No users found'. At the bottom, there is a log table with columns 'Time', 'Source', 'Severity', and 'Message'. The log entries are:

Time	Source	Severity	Message
21:56:08	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
21:56:49	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 25
21:56:58	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Удаленный сервер возвратил ошибку: (403) Запрещ...

At the bottom left, there are buttons for 'Settings', 'Deactivate AutoScroll', 'Clear', and 'Save log to File'. A status bar at the bottom says 'All searchers have finished'.

The screenshot shows the zapzap - FOCA Open Source 3.4.7.1 application window. On the left, there's a tree view of a project named 'zapzap' containing 'Network', 'Domains', 'Document Analysis' (with 'Files (0/55)' selected), 'Metadata Summary' (with 'Users (0)', 'Folders (0)', 'Printers (0)', 'Software (0)', 'Emails (0)', 'Operating Systems (0)', 'Passwords (0)', 'Servers (0)'), and 'Malware Summary (DIARIO)'. The main area features the Foca logo and a search bar with 'Custom search'. Below it is a table of search results:

ID	Type	URL	Download	Download Date	Size	Meta
9	pdf	https://cdn.zapier.com/storage/learn_ebooks/66c3a6e...	X	-	4.41 MB	X
10		https://zapier.com/apps/razorpay-1/integrations/pdfiller	X	-	-	X
11	html	https://community.zapier.com/get-help-50/index338.html	X	-	-	X
12		https://zapier.com/learn/google-sheets/how-to-use-goo...	X	-	208.97 KB	X
13		https://zapier.com/apps/123formbuilder/integrations	X	-	-	X
14	pdf	https://cdn.zapier.com/storage/learn_ebooks/4589266...	X	-	1.5 MB	X
15		https://community.zapier.com/featured-articles-65/autom...	X	-	-	X
16		https://zapier.com/apps/expensify/integrations/climate...	X	-	-	X
17		https://zapier.com/apps/timely/integrations/hellosign	X	-	-	X
18		https://zapier.com/apps/chatarchitect/integrations/click...	X	-	-	X
19		https://zapier.com/apps/clicksend/integrations/member...	X	-	-	X

Below the table is a log table:

Time	Source	Severity	Message
12:48:46	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 26
12:48:47	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
12:48:47	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Удаленный сервер возвратил ошибку: (403) Запрещ...

At the bottom are buttons for 'Settings', 'Deactivate AutoScroll', 'Clear', and 'Save log to File'.

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

Screenshot of the Censys.io interface showing the results for the IP address 200.115.173.167 (maria.telcorush.com). The interface includes a search bar, navigation tabs (Summary, Explore, History, WHOIS), and a map of Central America highlighting Panama.

**Basic Information:**

- OS: Red Hat Enterprise Linux 7
- Network: Cyber Cast International, S.A. (PA)
- Routing: 200.115.173.0/24 via AS27956
- Protocols: 21/FTP, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 143/IMAP, 443/HTTP, 465/SMTP, 587/SMTP, 993/IMAP, 995/POP3, 2077/HTTP, 2078/HTTP, 2079/HTTP, 2080/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2090/HTTP, 2091/HTTP, 2095/HTTP, 2096/HTTP, 2995/SSH, 3306/MYSQL, 10000/HTTP

**Software:**

- linux
- CPE: cpe:2.3:o\*:linux:\*\*\*\*\*:\*
- PureFTPD: Pure-FTPD
- CPE: cpe:2.3:a:pureftpd:pure-ftpd:\*\*\*\*\*:\*

**Details:**

Banner: 220----- Welcome to Pure-FTPD [privsep] [TLS] -----  
220>You are user number 1 of 50 allowed

**Results:**

Host Filters: Autonomous System (e.g., AMAZON-AES, AMAZON-02, MICROSOFT-CORP-MSN-AS-BLOCK, DIGITALOCEAN-ASN, WEBZILLA), Location (United States, Germany, Ireland, United Kingdom, Netherlands), Service Names (HTTP, SSH, SMTP, IMAP, FTP), Ports (e.g., 22, 25, 443, 53, 80, 110, 143, 2077, 2080, 2086, 2087, 2090, 2095, 2995, 3306).

Geographic Location: Country - Panama (PA), Coordinates - 9.0, -80.0, Timezone - America/Panama.

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

shodan.io search results for 'ZAPIER-WINDOWS' (2021-10-19T01:47:07.352038)

**TOP ORGANIZATIONS**

Organization	Count
Amazon Technologies Inc.	9
Amazon Data Services NoVa	4
GoDaddy.com, LLC	2
Amazon Data Services Ireland Limited	1
CustodianDC Limited	1

**TOP PRODUCTS**

Product	Count
nginx	14
Remote Desktop Protocol	3
Microsoft IIS httpd	1

**34.251.160.142** (2021-10-19T01:47:07.352038)

Target Name: ZAPIER-WINDOWS  
NetBIOS Computer Name: ZAPIER-WINDOWS  
NetBIOS Domain Name: ZAPIER-WINDOWS  
DNS Domain Name: zapier-windows  
FQDN: zapier-windows  
System Time: 2021-10-28 00:17:12.486401

**SSL Certificate**  
HTTP/1.1 404  
Issued By: DigiCert SHA2 Secure Server CA  
- Common Name: sup.km.symphony.com  
- Organization: Symphony Communication Services, LLC  
Supported SSL Versions: TLSv1.2

**Dovetail** (2021-10-19T01:45:06.270441)

34.200.165.14 (2021-10-19T01:45:06.270441)  
ec2-34-200-165-14.compute-1.amazonaws.com  
Amazon Technologies Inc.  
United States, Ashburn  
cloud

**SSL Certificate**  
HTTP/1.1 200 OK  
Issued By: Amazon  
- Common Name: \*.in2.dovetailapp.com  
- Organization: Amazon  
Supported SSL Versions: TLSv1.2

**34.82.227.151** (2021-10-19T00:17:12.578761)

151.227.82.34.bc.googleusercontent.com  
Google LLC  
United States, The Dalles  
cloud

Remote Desktop Protocol:  
OS: Windows 10/Windows Server 2019  
OS Build: 10.0.17763  
Target Name: ZAPIER-WINDOWS  
NetBIOS Domain Name: ZAPIER-WINDOWS  
NetBIOS Computer Name: ZAPIER-WINDOWS  
DNS Domain Name: zapier-windows  
FQDN: zapier-windows  
System Time: 2021-10-28 00:17:12.486401

**34.251.160.142** (2021-10-19T01:47:07.352038)

ec2-34-251-160-142.eu-west-1.compute.amazonaws.co m  
Amazon Data Services Ireland Limited  
Ireland, Dublin  
cloud

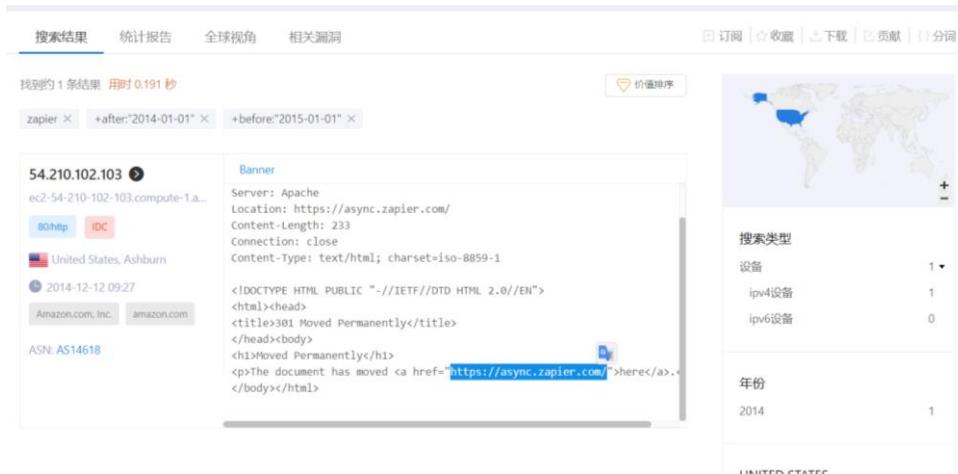
**SSL Certificate**  
HTTP/1.1 404  
Issued By: DigiCert SHA2 Secure Server CA  
- Common Name: sup.km.symphony.com  
- Organization: Symphony Communication Services, LLC  
Supported SSL Versions: TLSv1.2

Аналогично censys, shodan позволил получить информацию об адресах доменов пользователей компаний, 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

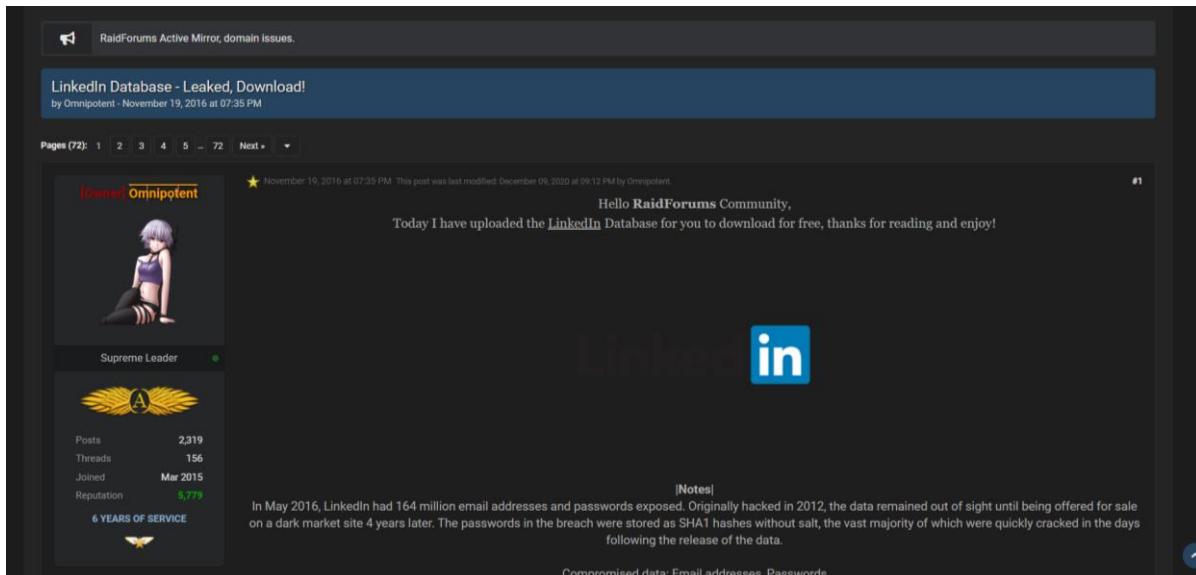
Search Results						
Post	Author	Forum	Replies	Views	Posted [asc]	
Thread: [ZAPIER ALTERNATIVE] PABBLY CONNECT LIFETIME DEAL PRIVATE DEAL LINK Post: [ZAPIER ALTERNATIVE] PABBLY CONNECT LIFETIME DEAL ... this is pabbly connect ( <a href="https://appsumo.me/Pabbly">https://appsumo.me/Pabbly</a> ) a Indian alternative to Zapier ( <a href="https://zapier.com">https://zapier.com</a> ) they run a special private campaign for LIFETIME deal <a href="https://i.imgur.com/WLNazU.png">https://i.imgur.com/WLNazU.png</a> https...	SHAMASH	General	1	344	April 06, 2021 at 02:13 AM	
Thread: Selz.io [Sendgrid - Office365 - Combo - RDP - SSH - Shells - Cpanels - And more] Post: RE: Selz.io [Sendgrid - Office365 - Combo - RDP - ... list of fresh premium account available in selz: <a href="https://www.selz.io">https://www.selz.io</a> <a href="http://sellthetrend.com">sellthetrend.com</a> <a href="https://heapsy.com">heapsy.com</a> <a href="https://similarweb.com">similarweb.com</a> <a href="https://commerceinspector.com">commerceinspector.com</a> <a href="http://ecomhunt.com">ecomhunt.com</a> <a href="http://nichecrawler.com">nichecrawler.com</a> <a href="http://zikanalytic...">zikanalytic...</a>	* Selz	General	42	6,190	March 31, 2021 at 07:15 PM	
Thread: Pull website info using Zapier Post: Pull website info using Zapier I found this to be very useful. Here's a quick guide to doing some really simple data extracting using some JavaScript with the Code module. <a href="https://tobico.net/post/2017/05/extracting-data-from...">https://tobico.net/post/2017/05/extracting-data-from...</a>	* johnsmithy365	Software	0	535	November 08, 2019 at 07:36 PM	
Thread: Netsparker 5.2.0.22027 exclusive for raidforums [PATCHED] Post: RE: Netsparker 5.2.0.22027 exclusive for raidforum... Fugitifer Wrote: (February 15, 2019 at 07:14 AM) – Yes because we can see the Changelog on your site! – From changelog: Code: – Netsparker 5.2.0.21893 - 18th December 2018 NEW FEATURES ...	mimao	Software	113	18,865	February 16, 2019 at 07:22 AM	
Thread: OSINT Links 6 Post: OSINT Links 6 263 Calendars and Scheduling Tool Link Assistant Bunchapp <a href="http://www.assistant.to">http://www.assistant.to</a> <a href="http://bunchapp.io">http://bunchapp.io</a> Calendly <a href="https://calendly.com">https://calendly.com</a> Cozi <a href="http://www.cozi.c...">http://www.cozi.c...</a>	Trigger	SE Tutorials	7	4,846	July 04, 2018 at 09:13 AM	

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.

The screenshot shows a user profile on a forum. The user has 10,608,493,955 records. They have been a Supreme Leader for 6 years. The user has 2,319 posts, 156 threads, and joined in March 2015. A list of datasets follows:

- [999,999,999 Records] | 2019 - (Collection) Multiple Collections (1 to 5+ AntiPublic + Zabbix + Myri) — Download Here! \* Download provided via Torrent
- [013,545,468 Records] | 2015 - (000webhost.com) 000Webhost Database — Download Here!
- [000,018,965 Records] | 2013 - (1337crew.to) 1337 Crew Database — Download Here!
- [000,000,586 Records] | 2014 - (745vpn.com) 143VPN Database — Download Here!
- [009,072,977 Records] | 2011 - (778.com) 178 Database — Download Here!
- [028,052,322 Records] | 2016 - (17.media) 17.Media (17 直播) Database — Download Here!
- [014,928,048 Records] | 2011 - (7k7k.com) 7k7k Database — Download Here!
- [000,782,609 Records] | 2016 - (abandonia.com) Abandonia Database — Download Here!
- [000,432,943 Records] | 2014 - (acme.org) Acme Database — Download Here!
- [152,445,165 Records] | 2013 - (adobe.com) Adobe Database — Download Here!
- [003,867,997 Records] | 2015 - (adultfriendfinder.com) Adult Friend Finder Database — Download Here!
- [000,166,380 Records] | 2014 - (animjunkies.com) Aim Junkies Database — Download Here!
- [000,132,788 Records] | 2015 - (alabama.gov) Alabama Voter Database — Download Here!
- [000,487,415 Records] | 2015 - (alaska.gov) Alaska Voter Database — Download Here!
- [000,200,257 Records] | 2016 - (allwomentalk.com) All Womens Talk Database — Download Here!
- [000,008,508 Records] | 2016 - (alphas.sx) Alphas.sx Forum Database — Download Here!
- [000,745,355 Records] | 2012 - (androidforums.com) Android Forums Database — Download Here!
- [000,170,707 Records] | 2016 - (animutank.com) Animu Tank Database — Download Here!
- [030,811,934 Records] | 2015 - (ashleymadison.com) Ashley Madison Database — Download Here!
- [000,088,871 Records] | 2015 - (autohotkey.com) Auto Hot Key (AHK) Database — Download Here!
- [000,422,959 Records] | 2014 - (avast.com) Avast Database — Download Here!
- [000,355,161 Records] | 2010 - (apple.com) Apple Database — Download Here!
- [000,026,554 Records] | 2017 - (forums.bandiananocogame.com) Bandai Namco Forums Database — Download Here!
- [000,530,270 Records] | 2011 - (battlefieldheroes.com) Battlefield Heroes Database — Download Here!
- [112,005,531 Records] | 2016 - (taobao.com) Badoo Database — Download Here!
- [001,022,883 Records] | 2014 - (thewebs.info) Bin Weevils Database — Download Here!
- [000,041,348 Records] | 2014 - (theshackles.com) RiteHacking Database — Download Here!



## 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.

Repository	Path	Count
RocketChat/Rocket.Chat	client/views/admin/integrations/IntegrationsPage.js	10 matches
withfig/autocomplete	src/zapier.ts	23 matches

The screenshot shows the GitHub README page for the `ZapierRestHooks` repository. At the top, there are status indicators for gem version (0.0.2), build (passing), maintainability (green), and test coverage (100%). Below these, a note states: "Rails engine that provides functionality for [Zapier REST hooks pattern](#)". A section titled "Installation" contains instructions to add the gem to the Gemfile and run the generator. A note at the bottom indicates that the generator will mount the engine in config/routes.rb at the path `/hooks`.

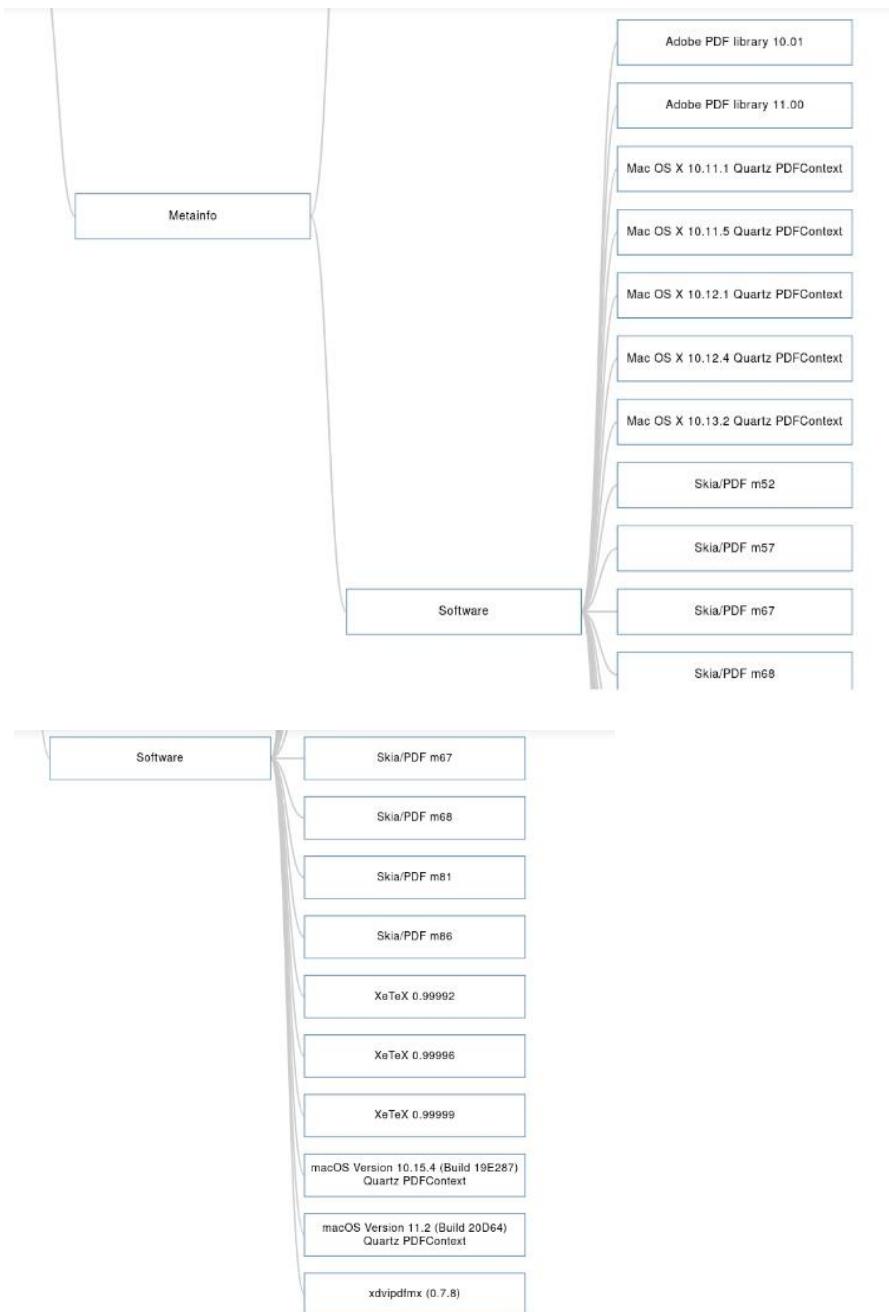
The screenshot shows the GitHub repository page for `esbanarango/zapier-REST-hooks`. The "Code" tab is selected. It displays a list of files and their last update times. The files listed are: app, bin, config, db/migrate, gemfiles, lib, and spec.

File	Description	Last Updated
app	Update rubocop	2 years ago
bin	Rails engine	5 years ago
config	Update rubocop	2 years ago
db/migrate	Update rubocop	2 years ago
gemfiles	Update rubocop	2 years ago
lib	Update rubocop	2 years ago
spec	Update rubocop	2 years ago

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

## 9. [github.com/yogeshojha/rengin](https://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.

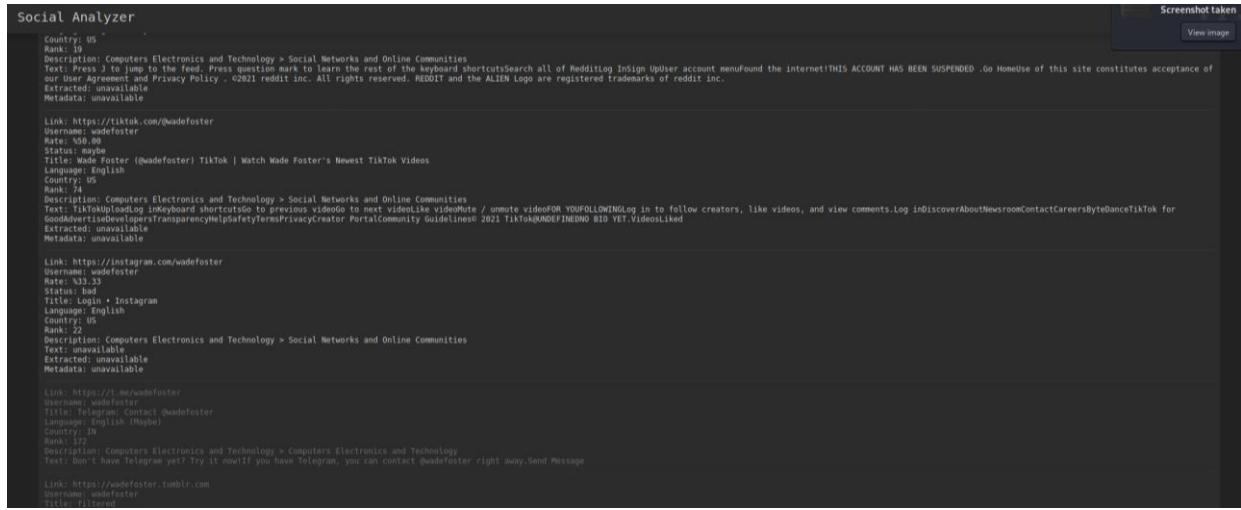


## 10. [github.com/qeeqbox/social-analyzer](https://github.com/qeeqbox/social-analyzer)

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

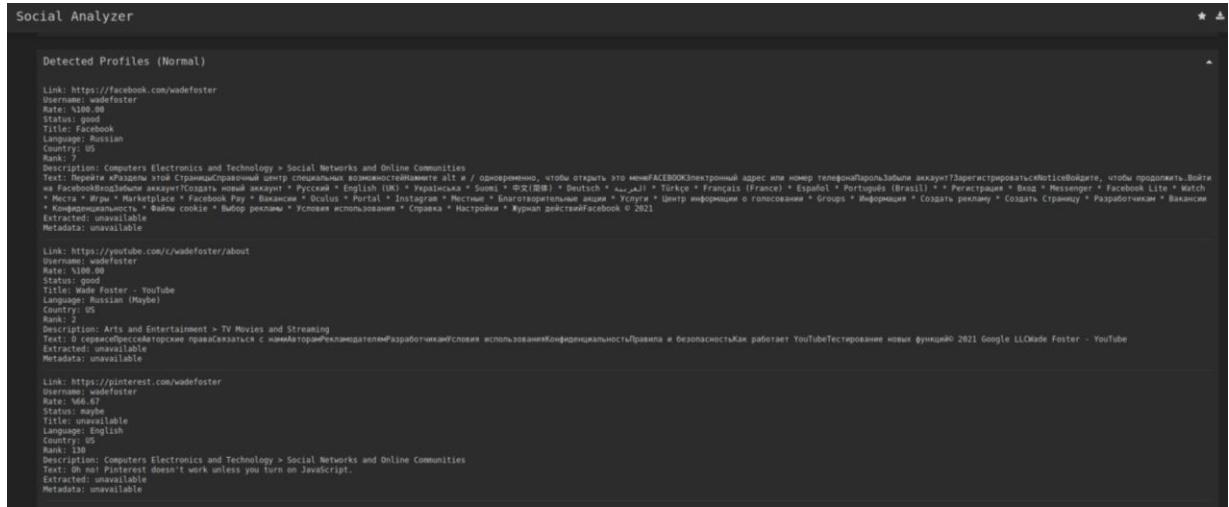
В числе которых:

# Wade Foster (Co-founder & CEO)



The screenshot displays the Social Analyzer tool interface with five sections, each showing profile information for 'wadefoster' on different platforms. The sections are: TikTok, Instagram, Facebook, YouTube, and Pinterest. Each section includes a 'Link', 'Username', 'Rate', 'Status', 'Title', 'Language', 'Country', 'Rank', 'Text', 'Extracted' (with a warning about unavailability), and 'Metadata'.

- TikTok:** Link: https://vt.tiktok.com/@wadefoster, Rate: 550.00, Status: maybe, Title: Wade Foster (@wadefoster) TikTok | Watch Wade Foster's Newest TikTok Videos, Language: English, Country: US, Rank: 5, Text: Press J to jump to the feed. Press question mark to learn the rest of the keyboard shortcuts, Search all of RedditLog InSign UpUser account menu found the internet! THIS ACCOUNT HAS BEEN SUSPENDED . Go Homeuse of this site constitutes acceptance of our User Agreement and Privacy Policy., ©2021 reddit inc. All rights reserved. REDDIT and the ALIEN Logo are registered trademarks of reddit inc., Extracted: unavailable, Metadata: unavailable
- Instagram:** Link: https://www.instagram.com/wadefoster, Rate: 553.35, Status: bad, Title: Wade Foster - Instagram, Language: English (English), Country: US, Rank: 23, Text: Description: Computers Electronics and Technology > Social Networks and Online Communities, Text: unavailable, Extracted: unavailable, Metadata: unavailable
- Facebook:** Link: https://facebook.com/wadefoster, Username: wadefoster, Rate: \$100.00, Status: good, Title: Wade Foster - Facebook, Language: Russian (Maybe), Country: US, Rank: 10, Text: Description: Computers Electronics and Technology > Social Networks and Online Communities, Text: Don't have a Telegram yet? Try it now! If you have Telegram, you can contact @wadefoster right away. Send Message, Extracted: unavailable, Metadata: unavailable
- YouTube:** Link: https://www.youtube.com/c/wadefoster/about, Username: wadefoster, Rate: \$100.00, Status: good, Title: Wade Foster - YouTube, Language: Russian (Maybe), Country: US, Rank: 1, Text: Description: Arts and Entertainment > TV Movies and Streaming, Text: Ooops! Please make sure you're logged into YouTube with the same account that you used to create your channel., Extracted: unavailable, Metadata: unavailable
- Pinterest:** Link: https://pinterest.com/c/wadefoster, Username: wadefoster, Rate: 138, Status: maybe, Title: unavailable, Language: English, Country: US, Rank: 138, Text: Description: Computers Electronics and Technology > Social Networks and Online Communities, Text: Oh no! Pinterest doesn't work unless you turn on Javascript., Extracted: unavailable, Metadata: unavailable



This screenshot shows the Social Analyzer tool interface with three sections: Facebook, YouTube, and Pinterest. The sections follow the same structure as the previous ones, displaying profile details for 'wadefoster' on these specific platforms.

- Facebook:** Link: https://facebook.com/wadefoster, Username: wadefoster, Rate: \$100.00, Status: good, Title: Wade Foster - Facebook, Language: Russian (Maybe), Country: US, Rank: 10, Text: Description: Computers Electronics and Technology > Social Networks and Online Communities, Text: Facebook uses cookies to provide you with a personalized experience. You can control what information you share on Facebook, including what information you receive from other people, as well as how others can interact with your profile., Extracted: unavailable, Metadata: unavailable
- YouTube:** Link: https://www.youtube.com/c/wadefoster/about, Username: wadefoster, Rate: \$100.00, Status: good, Title: Wade Foster - YouTube, Language: Russian (Maybe), Country: US, Rank: 1, Text: Description: Arts and Entertainment > TV Movies and Streaming, Text: Ooops! Please make sure you're logged into YouTube with the same account that you used to create your channel., Extracted: unavailable, Metadata: unavailable
- Pinterest:** Link: https://pinterest.com/c/wadefoster, Username: wadefoster, Rate: 138, Status: maybe, Title: unavailable, Language: English, Country: US, Rank: 138, Text: Description: Computers Electronics and Technology > Social Networks and Online Communities, Text: Oh no! Pinterest doesn't work unless you turn on Javascript., Extracted: unavailable, Metadata: unavailable



# Bryan Helwig (Co-founder & CTO)

Social Analyzer

Link: <https://facebook.com/BryanHelwig>  
Username: BryanHelwig  
Rate: \$100.00  
Status: good  
Title: Bryan Helwig  
Language: Russian  
Country: US  
Rank: 7  
Description: Computers Electronics and Technology > Social Networks and Online Communities  
Text: unavailable  
Extracted: unavailable  
Metadata: unavailable

Link: <https://instagram.com/BryanHelwig>  
Username: BryanHelwig  
Rate: \$100.00  
Status: good  
Title: Bryan Helwig (@bryanhelwig) • Instagram photos and videos  
Language: English  
Country: US  
Rank: 22  
Description: Computers Electronics and Technology > Social Networks and Online Communities  
Text: unavailable  
Extracted: unavailable  
Metadata: unavailable

Link: <https://reddit.com/user/BryanHelwig>  
Username: BryanHelwig  
Rate: \$100.00  
Status: good  
Title: bryanhelwig (u/bryanhelwig) - Reddit  
Language: English (Maybe)  
Country: US  
Rank: 31  
Description: Computers Electronics and Technology > Social Networks and Online Communities  
Text: Press J to jump to the feed. Press question mark to learn the rest of the keyboard shortcutsSearch all of RedditInSign UpUser account menuFound the internet!OverviewPostsCommentsAwards received  
Legacy/NewNewbie!TopNewbie!TopBryanHelwig commented onBUGS & ISSUES MEGATHREAD•Posted by51 points • 1 year agoUsing Xbox 360 controller, and the rudder is not analog. If I so much as slightly touch a controller trigger, the  
pedals fully go left, right, or plane pitches to the side like crazy...An I missing settings?•1 point bybryanhelwig commented onHUSHING EMAS AND GES•posted by2 points • 1 year ago  
can use the Code by Zapier action to execute 35. There is a similar answer on Stack Overflow: <https://stackoverflow.com/a/43477338#43477338>bryanhelwig commented onENT BUT YOUR GPU COMPUTE TO AI RESEARCHERS AND MAKE ~2X MORE  
THAN THESE WORDS2 points • 4 years agoThis is how it works... "I just want more GPUs so I can finish up my recurrent neural net chatbot trained on past text messages. But thank you for the kind  
words. Since over32 points • 4 years agoThis is how it works... "I just want to do cool thing X", but hidden within that is the fact that if you want it, maybe other people do too. Silly hobbies or toys become very serious.

Link: <https://pinterest.com/BryanHelwig>  
Username: BryanHelwig  
Rate: \$66.67

Social Analyzer

Link: <https://tiktok.com/@bryanhelwig>  
Username: BryanHelwig  
Rate: \$50.00  
Status: maybe  
Title: bryanhelwig (@bryanhelwig) TikTok | Watch bryanhelwig's Newest TikTok Videos  
Language: English (Maybe)  
Country: US  
Rank: 70  
Description: Computers Electronics and Technology > Social Networks and Online Communities  
Text: TikTok!plalog inKeyboard shortcutsGo to previous videoGo to next videoLike videoRate / unmute videoFOR YOUFOLLOWINGLog in to follow creators, like videos, and view comments.Log  
inDiscoverAboutNewsroomContactCareersByTeDanceTikTok forGoodAdvertiseDevelopersTransparencyHelpSafetyTermsPrivacyCreator PortalCommunity Guidelines© 2021 TikTokUNDEFINENO BIO YET.VideosLiked  
Extracted: unavailable  
Metadata: unavailable

Link: <https://t.me/BryanHelwig>  
Username: BryanHelwig  
Title: Telegram Contact @BryanHelwig  
Language: English (Maybe)  
Country: IN  
Rank: 1  
Description: Computers Electronics and Technology > Computers Electronics and Technology  
Text: Don't have Telegram yet? Try it now!If you have Telegram, you can contact @BryanHelwig right away.send Message

Link: <https://youtube.com/c/BryanHelwig/about>  
Username: BryanHelwig  
Title: filtered  
Language: unavailable  
Country: US  
Rank: 2  
Description: Arts and Entertainment > TV Movies and Streaming  
Text: filtered

Link: <https://BryanHelwig.tumblr.com>  
Username: BryanHelwig  
Title: filtered  
Language: English (Maybe)  
Country: US

Social Analyzer

Description: Computers Electronics and Technology > Social Networks and Online Communities

Link: <https://t.me/BryanHelmig>

Username: BryanHelmig

Title: Contact (@BryanHelmig)

Language: English (Maybe)

Country: IN

Rank: 1

Description: Computers Electronics and Technology > Computers Electronics and Technology

Text: Don't have Telegram yet? Try it now! If you have Telegram, you can contact @BryanHelmig right away. Send Message

Link: <https://youtube.com/c/BryanHelmig/about>

Username: BryanHelmig

Title: filtered

Language: unavailable

Country: US

Rank: 2

Description: Arts and Entertainment > TV Movies and Streaming

Text: filtered

Link: <https://BryanHelmig.tumblr.com>

Username: BryanHelmig

Title: filtered

Language: English (Maybe)

Country: US

Rank: 3

Description: Computers Electronics and Technology > Social Networks and Online Communities

Text: filtered

Logs

Cancel Open

## Jacob Sowels (Senior frontend)

Social Analyzer

Enter Profile Name

jacobssowles Find profiles in Fast mode (Recommended) or Fast Options Analyze Clear Reset

**Detected Profiles (Normal)**

Link: <https://facebook.com/jacobssowles>

Username: jacobssowles

Rate: 100.00

Status: good

Title: Jacob Sowles

Language: Russian

Country: US

Rank: 7

Description: Computers Electronics and Technology > Social Networks and Online Communities

Text: unavailable

Extracted: unavailable

Metadata: unavailable

Link: <https://instagram.com/jacobssowles>

Username: jacobssowles

Rate: 100.00

Status: good

Title: Jacob Sowles (@jacobssowles) • Instagram photos and videos

Language: English

Country: US

Rank: 8

Description: Computers Electronics and Technology > Social Networks and Online Communities

Text: unavailable

Extracted: unavailable

Metadata: unavailable

Cancel Open

## Filipa Lacerda (Senior frontend)

FilipaLacerda Find profiles in Fast mode (Recommended) or Fast Options Analyze Clear Reset

**Detected Profiles (Normal)**

Link: <https://facebook.com/FilipaLacerda>

Username: FilipaLacerda

Rate: 100.00

Status: good

Title: Facebook

Language: Russian

Country: US

Rank: 7

Description: Computers Electronics and Technology > Social Networks and Online Communities

Link: <https://www.facebook.com/filipalacerda> / или временно, чтобы открыть это на FACEBOOK Электронный адрес или номер телефона ярлык аккаунт? Зарегистрироваться с Notice в блоге, чтобы продолжить. Войти на FacebookВход в аккаунт? Создать новый аккаунт \* Русский \* English (UK) \* Українська \* Suomi \* 中文(简体) \* Deutsch \* اردو \* Türkçe \* Français (France) \* Español \* Português (Brasil) \* Регистрация \* Вход \* Messenger \* Facebook Lite \* Места \* Игры \* Marketplace \* Facebook Pay \* Вакансии \* Oculus \* Portal \* Instagram \* Несколько \* Благотворительные акции \* Услуги \* Центр информации о голосовании \* Groups \* Информация о группах \* Видео \* Реклама \* Создать страницу \* Разработчикам \* Вакансии \* Конфиденциальность \* Файлы cookie \* Выбор рекламы \* Условия использования \* Справка \* Настройки \* Курьер доставки Facebook © 2021

Text: unavailable

Extracted: unavailable

Metadata: unavailable

Link: <https://Instagram.com/FilipaLacerda>

Username: FilipaLacerda

Rate: 100.00

Status: good

Title: filipalacerda profile on Instagram • 465 posts

Language: English

Country: US

Rank: 8

Description: Computers Electronics and Technology > Social Networks and Online Communities

Text: unavailable

Extracted: unavailable

Metadata: unavailable

Cancel Open

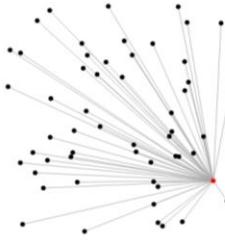
## 11. [github.com/smicallef/spiderfoot](https://github.com/smicallef/spiderfoot)

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

### Zapier FINISHED

Summary Browse Graph Scan Settings Log

R F G C D



Create a (free) SpiderFoot HX account in seconds and try it out for yourself.

### Zapier FINISHED

Summary Browse Graph Scan Settings Log

R F G C D

```

● FurAffinity (Category: XXXPORNOXXX) <SFURL>https://www.furaffinity.net/user/Zapier</SFURL>
● Hamster (Category: XXXPORNOXXX) <SFURL>https://hamster.com/users/Zapier</SFURL>
● Internet Archive User Search (Category: misc) <SFURL>https://ia
● eto (Category: (category) (category)) <SFURL>https://www.eto.com/categories/</SFURL>
● Chess.com (Category: gaming) <SFURL>https://www.chess.com/member/Zapier</SFURL>
● slideshare (Category: social) <SFURL>https://www.slideshare.net/Zapier</SFURL>
● WordPress Support (Category: blog) <SFURL>https://wordpress.org/support/users/Zapier/</SFURL>

```

Create a (free) SpiderFoot HX account in seconds and try it out for yourself.

Также, данный инструмент позволил получить профиль Bryan Helwig на hacker news и codementor.

SpiderFoot v3.4.0 | Profile: bryanh | Hacker | + | Screenshot taken | View image

https://news.ycombinator.com/user?id=bryanh

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Hacker News new | past | comments | ask | show | jobs | submit login

user: bryanh  
created: March 7, 2010  
karma: 4832  
about: co-founder/cto zapier.com (YC S12) writes at bryanhelwig.com

I likes to hack and play the jazz.  
bryanATzapierDOTcom

[ my public key: https://keybase.io/bryanhelwig; my proof: https://keybase.io/bryanhelwig/sigs/pnTRoKoMXhpYlLmY4mswphckt5p2R0jHZHrxa9Elg ]

[submissions](#) [comments](#) [favorites](#)

Bryan Helwig

ABOUT ME

Tijuana (-07:00)

Указан предполагаемый часовой пояс.

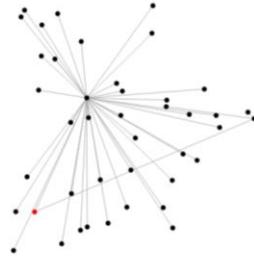
spiderfoot New Scan Scans Settings

Dark Mode  About

bryanhelmig RUNNING

Summary Browse Graph Scan Settings Log

R F PDF CSV JSON Download



spiderfoot New Scan Scans Settings

Dark Mode  About

bryanhelmig FINISHED

Summary Browse Graph Scan Settings Log

CSV JSON Download Search... 🔍

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	37	37	2021-10-23 02:19:58
Human Name	1	1	2021-10-23 02:19:20
PGP Public Key	1	1	2021-10-23 02:19:21
Raw Data from RIRs/APIs	1	1	2021-10-23 02:19:21
Search Engines Web Content	2	2	2021-10-23 02:19:23
Social Media Presence	2	2	2021-10-23 02:19:21
Username	2	2	2021-10-23 02:19:20

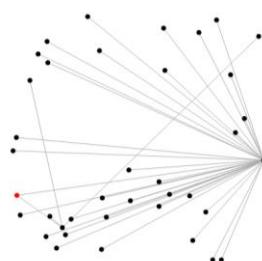
spiderfoot New Scan Scans Settings

Dark Mode  About

Wade RUNNING

Summary Browse Graph Scan Settings Log

R F PDF CSV JSON Download



Check out our YouTube channel to see SpiderFoot HX in action.

*Граф Wade Foster. Какой-либо ярусу информации найдено не было.*

## 12. github.com/laramies/theHarvester

```
(kali㉿kali)-[~/theHarvester]
$ theHarvester -d zapier.com -l 300 -b bing
*****
* [I] [L] [C] [A] [V] [E] [X] [P] [D] [B] [H] [F] [G] [M] [N] [O] [S] [T] [R] [U] [W] [Y] *
* theHarvester 4.0.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
```

[\*] Target: zapier.com  
Searching 0 results.  
[\*] Searching Bing.  
[\*] No IPs found.  
[\*] Emails found: 2

contact@zapier.com  
shipping123@robot.zapier.com

[\*] Hosts found: 12

api.zapier.com:65.9.42.73, 65.9.42.51, 65.9.42.105, 65.9.42.98  
cdn.zapier.com:143.204.73.77, 143.204.73.102, 143.204.73.84, 143.204.73.115  
community.zapier.com:13.249.162.117, 13.249.162.8, 13.249.162.9, 13.249.162.96  
developer.zapier.com:13.249.162.35, 13.249.162.81, 13.249.162.31, 13.249.162.22  
go.zapier.com:13.225.159.98, 13.225.159.27, 13.225.159.88, 13.225.159.65  
maker.zapier.com:54.157.58.70, 52.204.242.176, 54.162.128.250, 18.205.36.100  
parser.zapier.com:54.87.109.243, 3.231.76.203  
platform.zapier.com:18.65.191.70, 18.65.191.49, 18.65.191.94, 18.65.191.76  
robot.zapier.com  
status.zapier.com:13.225.159.15, 13.225.159.124, 13.225.159.13, 13.225.159.46  
store.zapier.com:54.209.91.188, 75.101.184.39, 54.221.251.148, 54.204.238.15  
workflows.zapier.com:143.204.73.45, 143.204.73.36, 143.204.73.123, 143.204.73.12

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

## 13. github.com/zricethezav/gitleaks

```
(kali㉿kali)-[~]
$ gitleaks --repo-url=https://github.com/zapier/zapier-platform --v
INFO[0000] cloning... https://github.com/zapier/zapier-platform
Enumerating objects: 24741, done.
Counting objects: 100% (24741/24741), done.
Delta compression using up to 8 threads
Compressing objects: 100% (548/548), done.
Total 24741 (delta 1010), reused 1198 (delta 935), pack-reused 23225
{
    "line": "AWSAccessKeyId: 'AKIAIKIAAKIAKIAKIA',",
    "lineNumber": 36,
    "offender": "AKIAIKIAAKIAKIAKIA",
    "offenderEntropy": "-1",
    "repo": "https://github.com/zapier/zapier-platform",
    "repoURL": "https://github.com/zapier/zapier-platform",
    "leakURL": "https://github.com/zapier/zapier-platform/blob/2847735eeddc618a0f59203e4ef2832703426d/packages/zapier-platform-core/test/tools/mocky.js#L36",
    "text": "AWSAccessKeyId",
    "commitMessage": "let there be light\n",
    "author": "Bryan Helmig",
    "email": "bryan@zapier.com",
    "filePath": "packages/zapier-platform-core/test/tools/mocky.js",
    "date": "2016-10-15T17:05:47Z",
    "tags": "key, AWS"
}
INFO[0088] scan time: 1 minute 5 seconds 984 milliseconds 686 microseconds
INFO[0088] commits scanned: 2998
WARN[0088] leaks found: 1
```

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.

```
31
32  const fakeSignedPostData = {
33    url: 'http://s3-fake.zapier.com/',
34    fields: {
35      policy: 'bm8gZHhbWE=',
36      AWSAccessKeyId: 'AKIAKIAKIAKIAKIAKIA',
37      acl: 'public-read',
38      key: 'some-route/d362f087-1106-4847-9261-669ec340b580',
39      signature: 'c4GzkaCtrc0ruvbZh6aSmf1k='
40    }
41  };
```

## 14. [github.com/sherlock-project/sherlock](https://github.com/sherlock-project/sherlock)

```
└─(kali㉿kali)-[~/sherlock]
$ python3 sherlock BryanHelmig 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 Zapierowels
[*] Checking username Zapierowels 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](https://github.com/s0md3v/Photon)

```

└─(kali㉿kali)-[~/Photon]-network strings
$ python3 photon.py -u zapier.com
          _              _       _   _ _ _ _ 
         | \_ \ _ \ / / \_ \ _ \ | \_ \ 
        / / / \_ \ / / / \_ \ / / / \_ \ v1.3.2
          | \_ \ / / \_ \ / / \_ \ / / \_ \ / / \_ \ / / \_ \ v1.3.2

[*] URLs retrieved from robots.txt: 19
[+] URLs retrieved from sitemap.xml: 29
[-] Level 1: 46 URLs

```

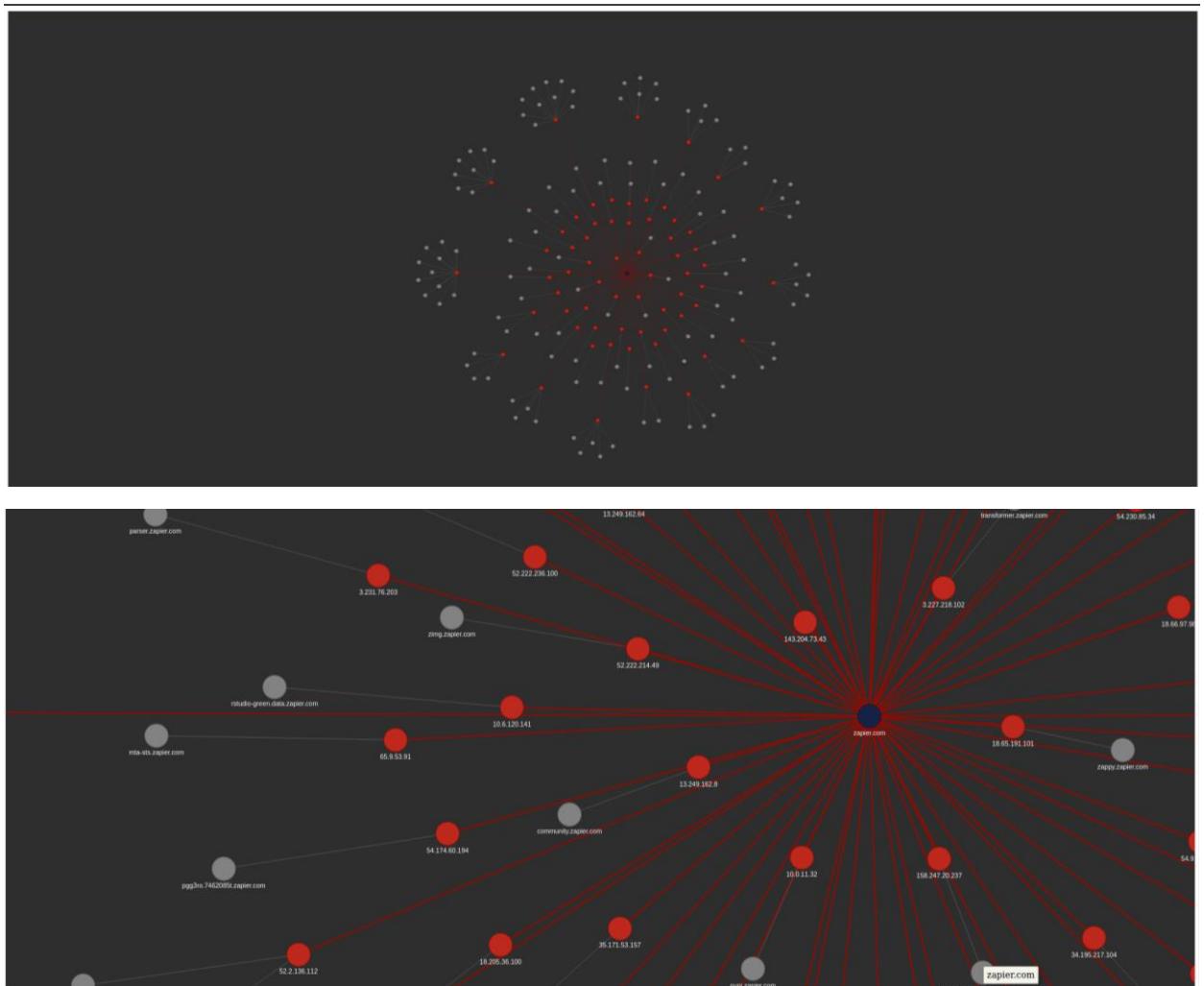
Информация (именно – поддомены компании), предоставленная данным сервисом, едва ли может считаться полезной, поскольку схожие ведения уже были предоставлены иными средствами.

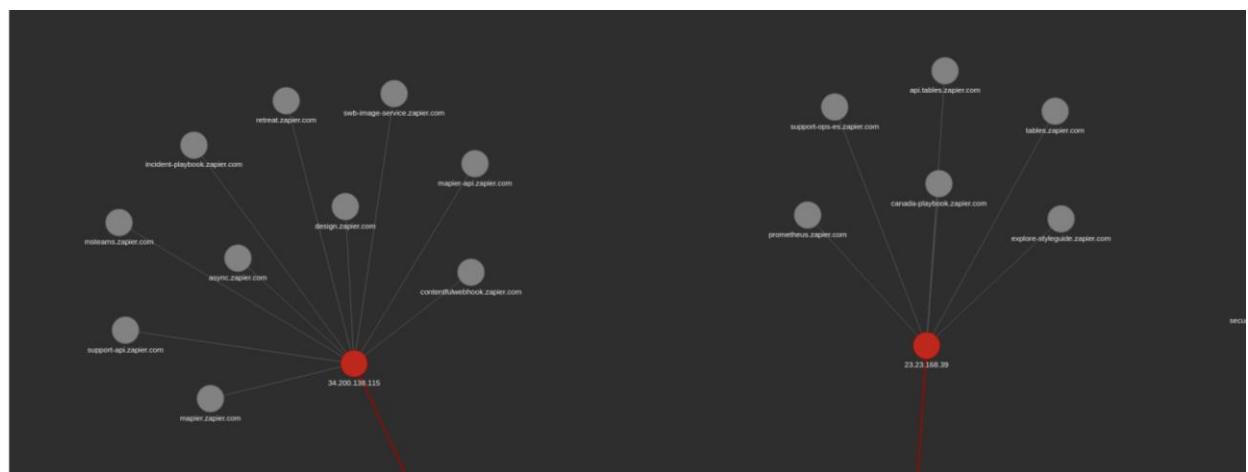
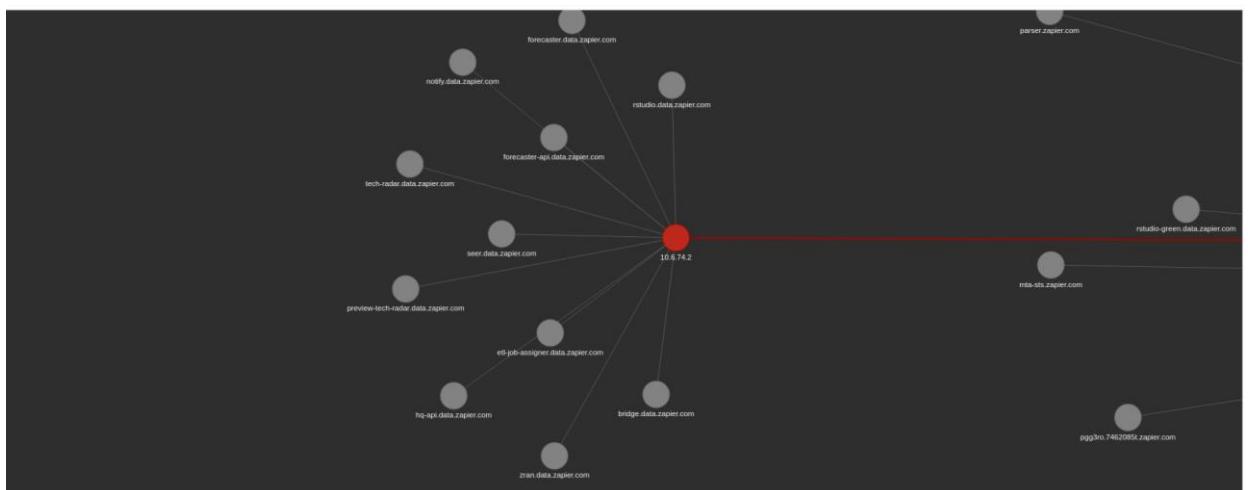
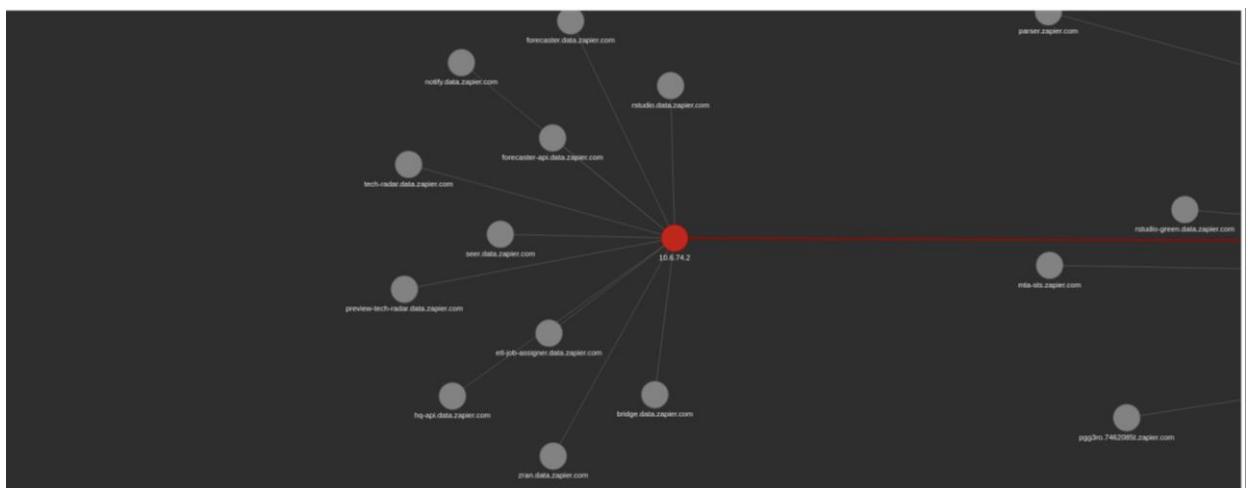
## 16. ahmia.fi

The screenshot shows a search results page for the query "zazie". The top navigation bar includes links for "About Ahmia", "Statistics", "Add Service", "IP search", "Contact", and "Blacklist". Below the search bar, it says "Any Time ▾" and "Did you mean [zazie](#)?". It notes "Omitted very similar entries. Displaying 2 matches in 0.31 seconds. Page 1 of 1." The first result is a link titled "Many feed readers don't handle plain text with XML-entities correctly" with the URL "Plain text isn't HTML. Many clients decode it as XML and then strip away the resulting HTML anyway. The spec is clear, but many implementations are buggy." The second result is a link titled "overview for Nexus2011" with the URL "No description provided".

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](https://github.com/screetsec/Sudomy)



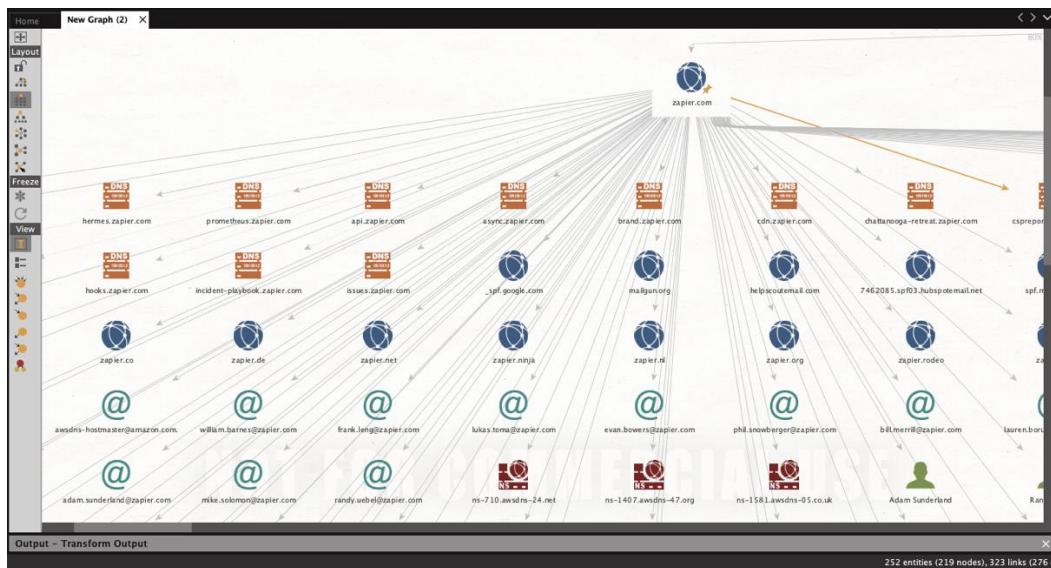




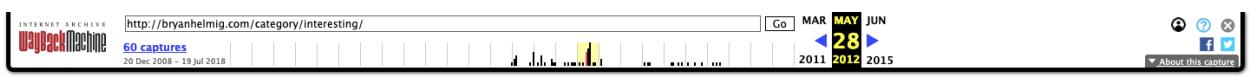
По результатам исследования были получены имена поддоменов Zapier.

## 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 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.



**Bryan Helmig**  
...does nerdy things.

**Notorious B.I.G's Crack Commandments In Business**  
Filed under: Interesting — Bryan on Feb 5th, 2010 @ 5:22 pm

In case you need a refresher, check out the tune here. While some are a stretch, a few are really quite relevant.

**1. Never let no one know how much dough you hold.**  
Keep your finances (good or bad) to yourself.  
Don't make the mistake of bragging about how well or mentioning how badly you're doing unless you have a very good reason for it. What you think of as idle talk amongst friends can get around very quickly and can affect future deals or relationships. When it comes to finances, its just better to keep your mouth shut.

**2. Never let 'em know your next move.**  
Keep your core strategies/opportunities under wraps.  
I know its tempting to talk about your plans or techniques, but just like #1, sometimes it's just best to shut up. Biggie elaborates on this with "don't you know Bad Boys move in silence or violence" which is just another way of letting you know that the big dogs don't over-plan and discuss, and they act.

**3. Never trust nobady.**  
Words are words. Get a contract.  
Trust is a funny and terribly fragile thing. While your business partners or clients may not want to ruin you from the outset, who knows what the future will bring? You need to protect yourself. Hire a lawyer, get a contract. Live by this motto: "**Everybody signs something.**"

**4. Never get high, on your own supply.**  
Discover the customers' needs; don't substitute your own.  
While you may think you have it under control, your customer should come first. They are the ones controlling your paycheck. Don't forget that. If you think you have all the answers, be prepared to fail. Badly.

about bryan  
  
bryan is a jazz and blues guitarist, small-time designer, python hacker, entrepreneur, and lover of fine whiskeys. he's the man behind such sites as [zapier](#), [bitbuffet](#) and [rankiac](#).  
we highly suggest following him on twitter or subscribing to the rss feed!

search:

pages  
about me  
bother me

and so on  
best guitar  
blues lick collection  
django help desk  
free guitar lessons  
glass cannon  
my facebook  
my linkedin  
my twitter

categories:

## 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](mailto:bryan@zapier.com) – корпоративная почта

[bryan@bryanhelmig.com](mailto:bryan@bryanhelmig.com) – личная почта

[bryanhelmig@gmail.com](mailto: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](mailto: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](mailto:mike@zapier.com) – корпоративная почта

[mikeknoop@gmail.com](mailto:mikeknoop@gmail.com) – личная почта

@mikeknoop – instagram



### **Olmo Maldonado (Sr. Engineer, Backend)**

<https://github.com/ibolmo>

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

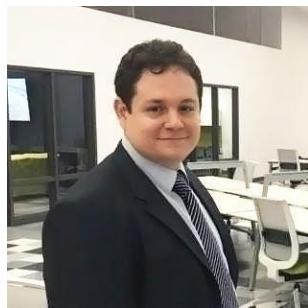
<https://www.facebook.com/ibolmo>

<https://twitter.com/ibolmo>

<http://ibolmo.com> – личный сайт

[me@ibolmo.com](mailto: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](mailto:jrsowles@gmail.com) – личная почта



### **Filipa Lacerda (Sr. Engineer, Frontend)**

<https://github.com/filipalacerda>

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

<https://twitter.com/FilipaLacerda>

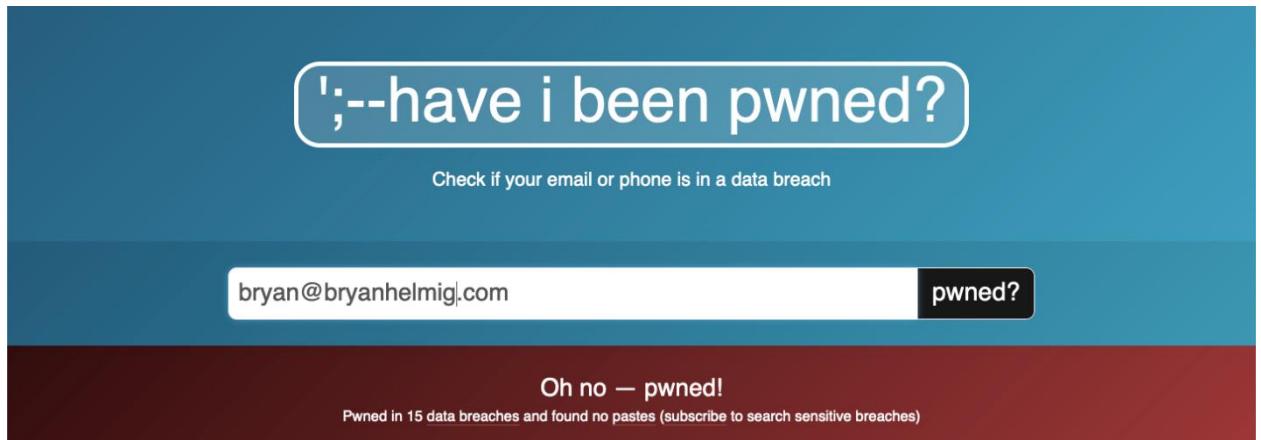
[lacerda.filipa@gmail.com](mailto:lacerda.filipa@gmail.com) – личная почта



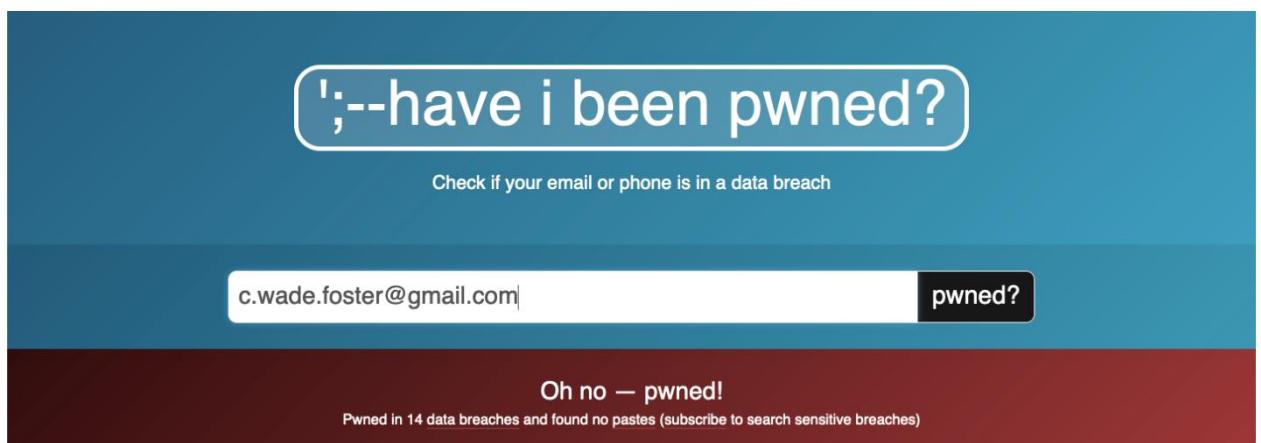
## **Изучение потенциальных жертв фишинговой атаки**

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 Helwig*



Личная почта, принадлежащая *Wade Foster*

# ';--have i been pwned?

Check if your email or phone is in a data breach

mikeknoop@gmail.com

pwned?

Oh no — pwned!

Pwned in 17 data breaches and found no pastes (subscribe to search sensitive breaches)

Личная почта, принадлежащая Mike Knoop

# ';--have i been pwned?

Check if your email or phone is in a data breach

me@ibolmo.com

pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Личная почта, принадлежащая Olmo Maldonado

# ';--have i been pwned?

Check if your email or phone is in a data breach

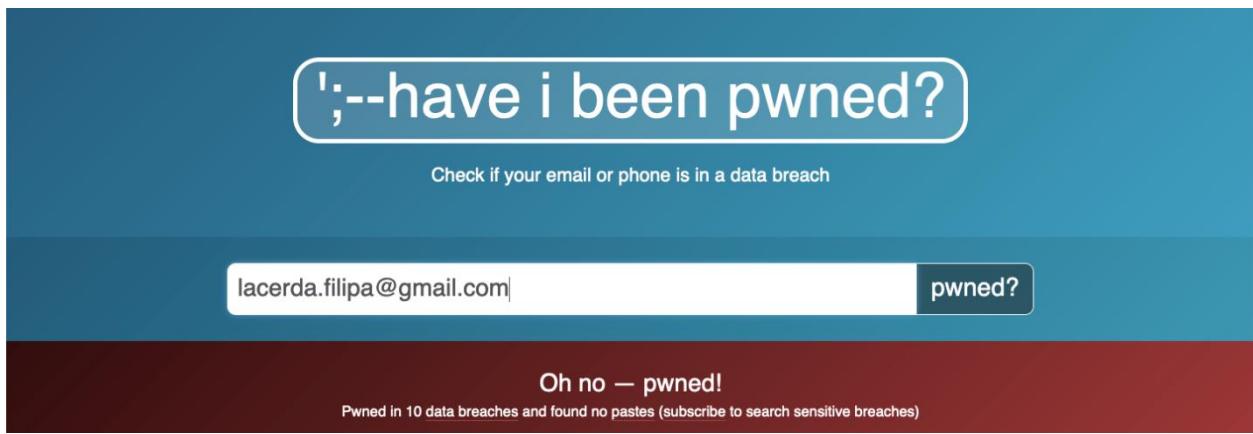
jrsowles@gmail.com

pwned?

Oh no — pwned!

Pwned in 11 data breaches and found no pastes (subscribe to search sensitive breaches)

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](mailto:@bryanhelmig.com) и [@ibolmo.com](mailto:@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.

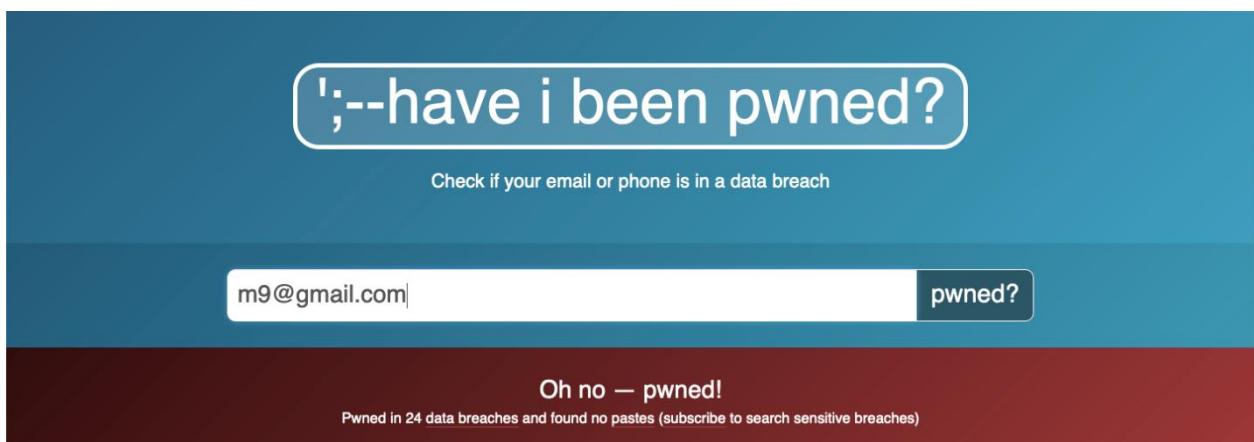
На личной странице Bryan Helmig в Facebook присутствуют ссылки на его сестру – Shelley Marie Helmig (<https://www.facebook.com/shelley.helmig>), а также на мать – Cheryl Helmig (<https://www.facebook.com/cheryl.helmig>).

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 сожалению, 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 количеством 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 (@michellewknop), был найден через функцию отметок на фото в Instagram. Через попытку сброса пароля была найдена её личная почта – [m9@gmail.com](mailto: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 Helwig и Mike Knoor, 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 слияниям 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/>