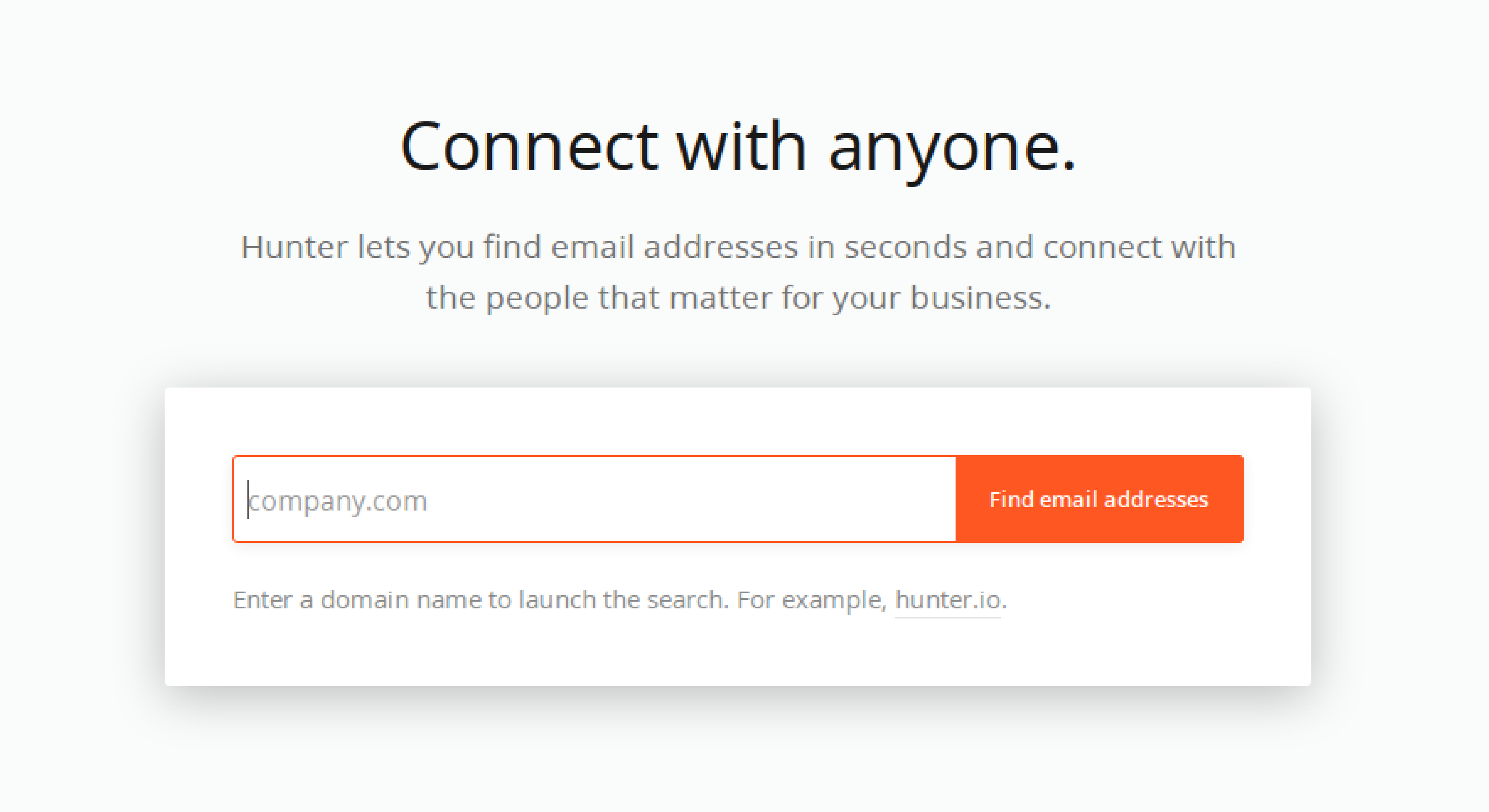
12 OSINT Resources For E-mail Addresses

17th September 2019 Nixintel OSINT Leave a Comment



Connect with anyone.

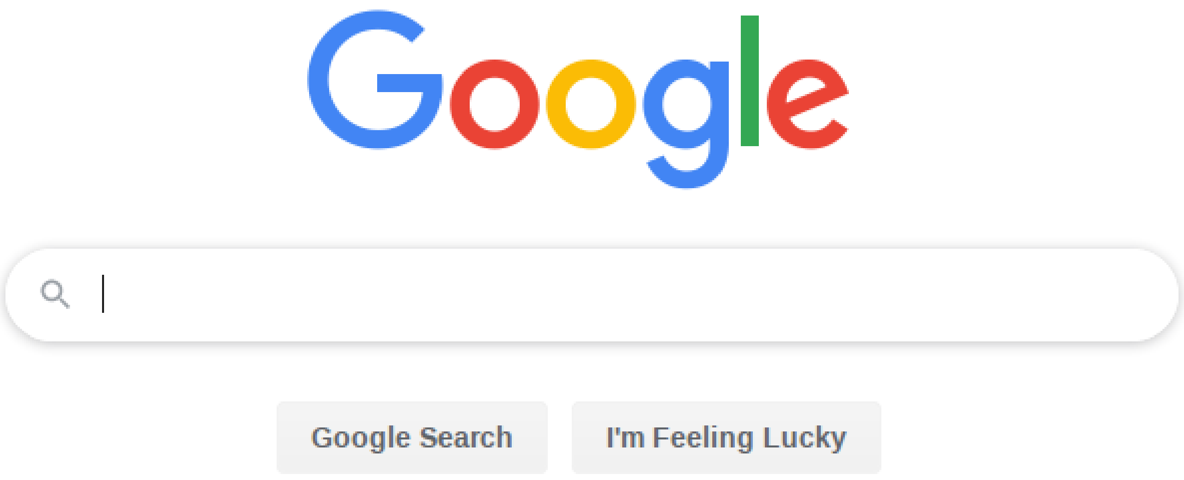
Hunter lets you find email addresses in seconds and connect with the people that matter for your business.

Enter a domain name to launch the search. For example, hunter.io.

Most OSINT investigations involve an e-mail address at some point. Some start with an e-mail and nothing else. E-mail addresses can sometimes be a bit of a challenge but they can also provide a wealth of information about a subject. The rest of this post will look at a range of different tools and techniques that can be used to get the most from an e-mail address.

The amount of information available about a particular e-mail address can vary widely. This depends on a number of different factors, such as how old the e-mail address is, how widely the owner has published it on the internet, and whether the provider is a common e-mail provided like Gmail or Protonmail, or whether the e-mail address is tied to its own company domain name.

1. Google



Google is as good a place as any to start a search, but sometimes it can be of surprisingly limited value for finding e-mail addresses. The main reason for this is that the places where people use their e-mail addresses (such as account login pages) are not accessible to Google. Nevertheless there are still some useful ways to find e-mail addresses where Google has indexed them.

Use quotation marks to return exact matches only. Searching for **"user@domain.com"** is more precise than searching for just **user@domain.com**.

The **intext** search modifier can also be used to find webpages where the e-mail address appears as a string. This can be particularly effective when combined with the site: modifier to search within the website of a company that your target is associated to. For example **site:targetcompany intext:target@email.com** is much more likely to be successful than just a hit-and-hope search. You could even tweak this technique to find a whole host of e-mail addresses associated to your target's organisation with the following search term

site:organisation.com intext:@organisation.com

This would return all indexable e-mail addresses within the company's website. This example shows you can use the following query to find all the e-mail addresses listed within the **bbc.co.uk** domain:

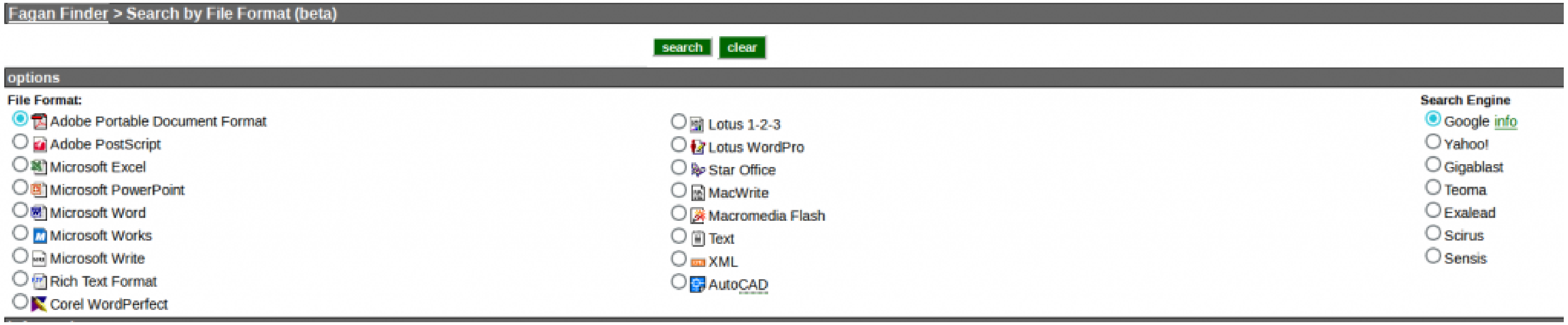
site:bbc.co.uk intext:@bbc.co.uk

Another really effective technique is to use the **filetype:** search operator find where your target's e-mail address. This can find a target's e-mail address hidden away inside PDF or other file types. This can reveal company documents, invoices, meeting minutes, sports club fixtures or any other kind of document. For example a search like:

intext:"boris.johnson.mp@parliament.uk" filetype:pdf

Will find any PDFs containing Boris Johnson's parliamentary e-mail address.

It’s particularly effective when searching for e-mails linked to organisations that have a lot of documents available on the web, such as government institutions or universities.



Fagan Finder > Search by File Format (beta)

options

File Format:

● Adobe Portable Document Format
○ Adobe PostScript
○ Microsoft Excel
○ Microsoft PowerPoint
○ Microsoft Word
○ Microsoft Works
○ Microsoft Write
○ Rich Text Format
○ Corel WordPerfect
○ Lotus 1-2-3
○ Lotus WordPro
○ Star Office
○ MacWrite
○ Macromedia Flash
○ Text
○ XML
○ AutoCAD

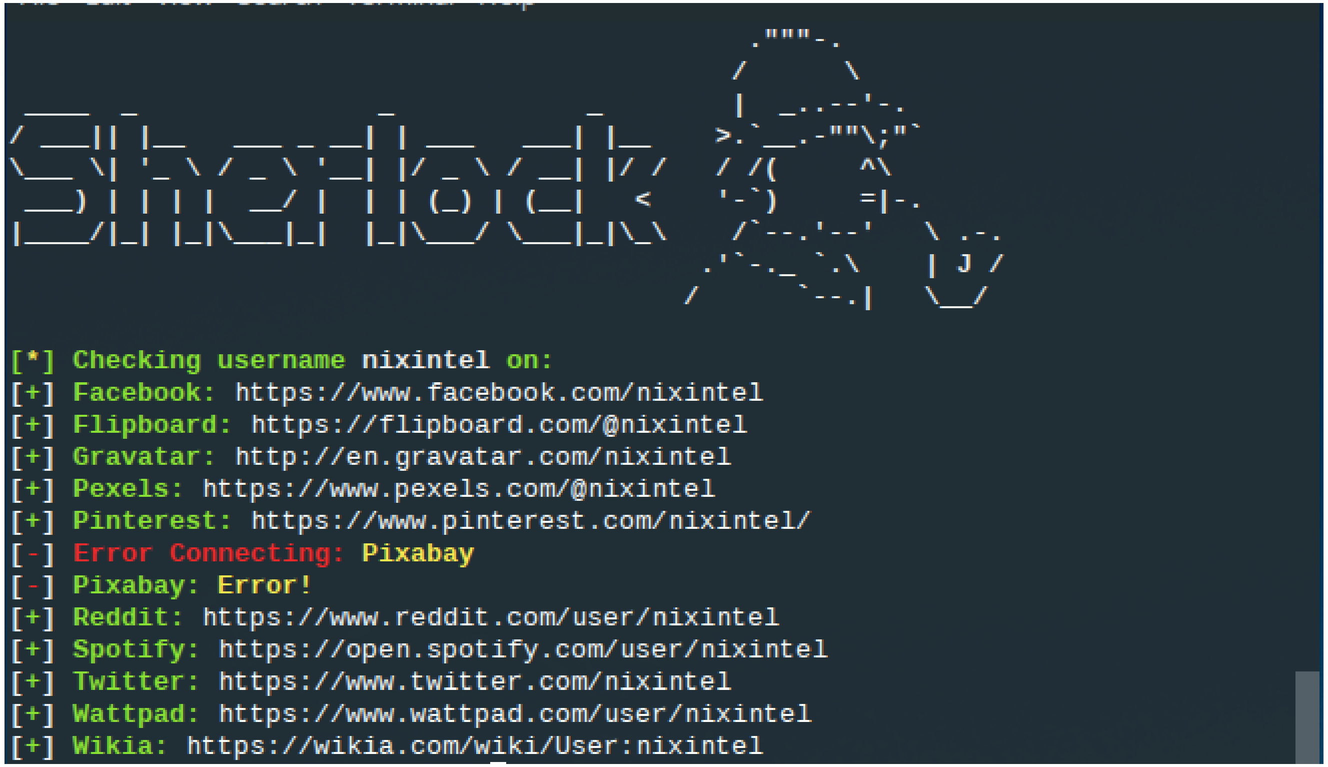
Search Engine

● Google info
○ Yahoo!
○ Gigablast
○ Teoma
○ Exalead
○ Scirus
○ Sensis

It’s also worth mentioning FaganFinder at this point. It works in a similar way to the Google filetype: search but it allows to combine different file types with a wider range of search engines.

2. Username

There’s often a link between someone’s e-mail address and their usernames. A good technique to try is to take the first part of a subject’s e-mail address and run it through a number of username search engines. So if you were trying to find out about more about **cryptoscammer666@gmail.com,** you’d target the username **cryptoscammer666.** The more unique an e-mail handle is, the more likely it is you’ll find a match. There are a number of browser based tools that can do this, but my favourite tool by far is Sherlock (set up and usage guide here).

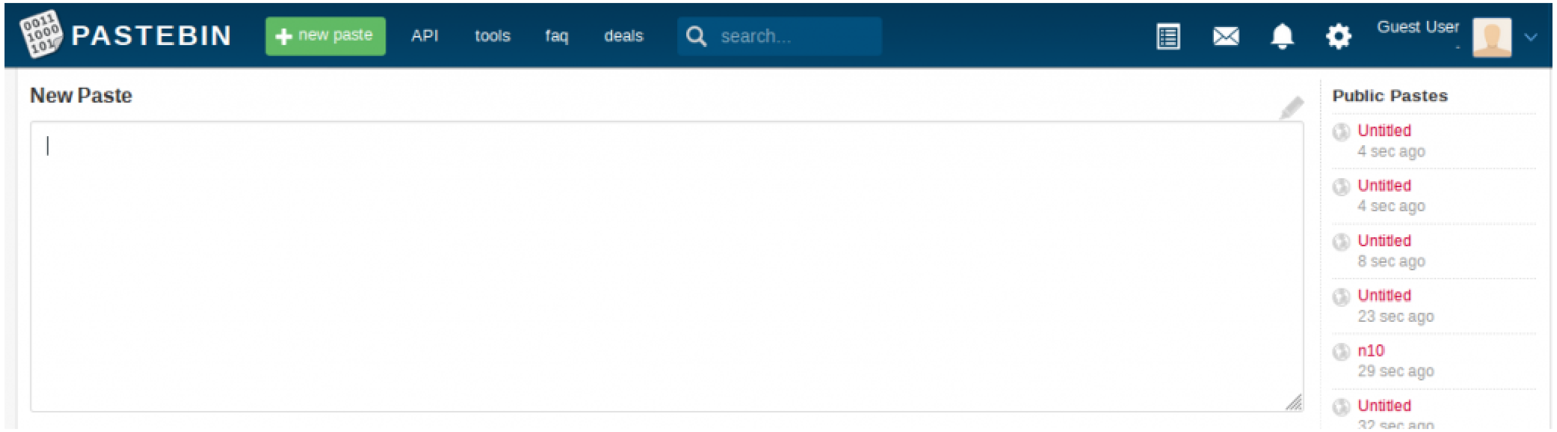


```
                                              ."""-.
                                             /      \
 ____  _               _            _        |  _..--'-.
/ ___|| |__   ___ _ __| | ___   ___| | __    >.`__.-""\;"`
\___ \| '_ \ / _ \ '__| |/ _ \ / __| |/ /    / /(     ^\
 ___) | | | |  __/ |  | | (_) | (__|   <     '-`)     =|-.
|____/|_| |_|\___|_|  |_|\___/ \___|_|\_\     /`--.'--'   \ .-.
                                            .'`-._ `.\    | J /
                                           /      `--.|   \__/

[*] Checking username nixintel on:
[+] Facebook: https://www.facebook.com/nixintel
[+] Flipboard: https://flipboard.com/@nixintel
[+] Gravatar: http://en.gravatar.com/nixintel
[+] Pexels: https://www.pexels.com/@nixintel
[+] Pinterest: https://www.pinterest.com/nixintel/
[-] Error Connecting: Pixabay
[-] Pixabay: Error!
[+] Reddit: https://www.reddit.com/user/nixintel
[+] Spotify: https://open.spotify.com/user/nixintel
[+] Twitter: https://www.twitter.com/nixintel
[+] Wattpad: https://www.wattpad.com/user/nixintel
[+] Wikia: https://wikia.com/wiki/User:nixintel
```

Just a note of caution though. Attribution and association of usernames is far from certain. Just because two accounts or e-mail addresses have the same username doesn't mean they're linked. Further corroboration should be done where possible. In the picture above, I found multiple online accounts with the username "nixintel" – but only one is actually me!

3. Pastes



Pastes are a treasure trove of OSINT information. They contain data breaches, public records, chatroom logs, and dozens of other kinds of useful information – including e-mail addresses. Pastebin is by far the most widely-used and has its own built in search engine.

NetBootCamp also has a custom search tool that allows you to search simultaneously across multiple paste sites.

Paste Site Search

Facebook Tool | Website Investigation Tool

SEARCH SEARCH FILTERS RESOURCES

Search Paste Sites with Filters

Google CSE filters are unreliable, but here is the date filter.
Keyword suggestions below. URL parameters are located here.

Search Term(s)

Numeric Value i.e. 1 | -Select Date Type ▾ | GO

Keyword Filters by Search Type

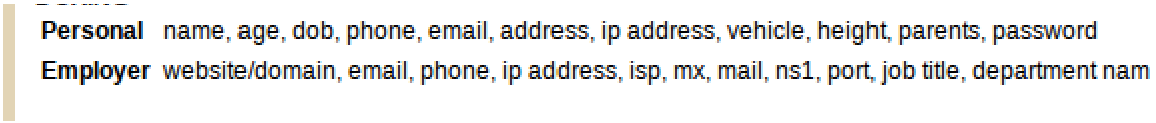
PIRACY

Video	x264, xvid, cam, scr, rip, hdtv, cam, ts, webrip, subs, torrent, nfo, French (language),-trailer, -soundtrack
Music	mp3, kpbs, m4a, aac
Games	serial key, mod, crack, ntsc
Software	repack, preactivated, crack, nulled
eBooks/Images	pdf, ebook, res, set, hd, pic

WEBSITES

HTML	javascripts, css, widgets, themes, author, blogger, screen name
Analytics	google analytics "ua-12345...", statcounter, histats
Publishers	google adsense "ca-pub...", widgets, i.e. sharethis id
Hosting	domain, ip address, ns, mx, isp, sql

DOXING

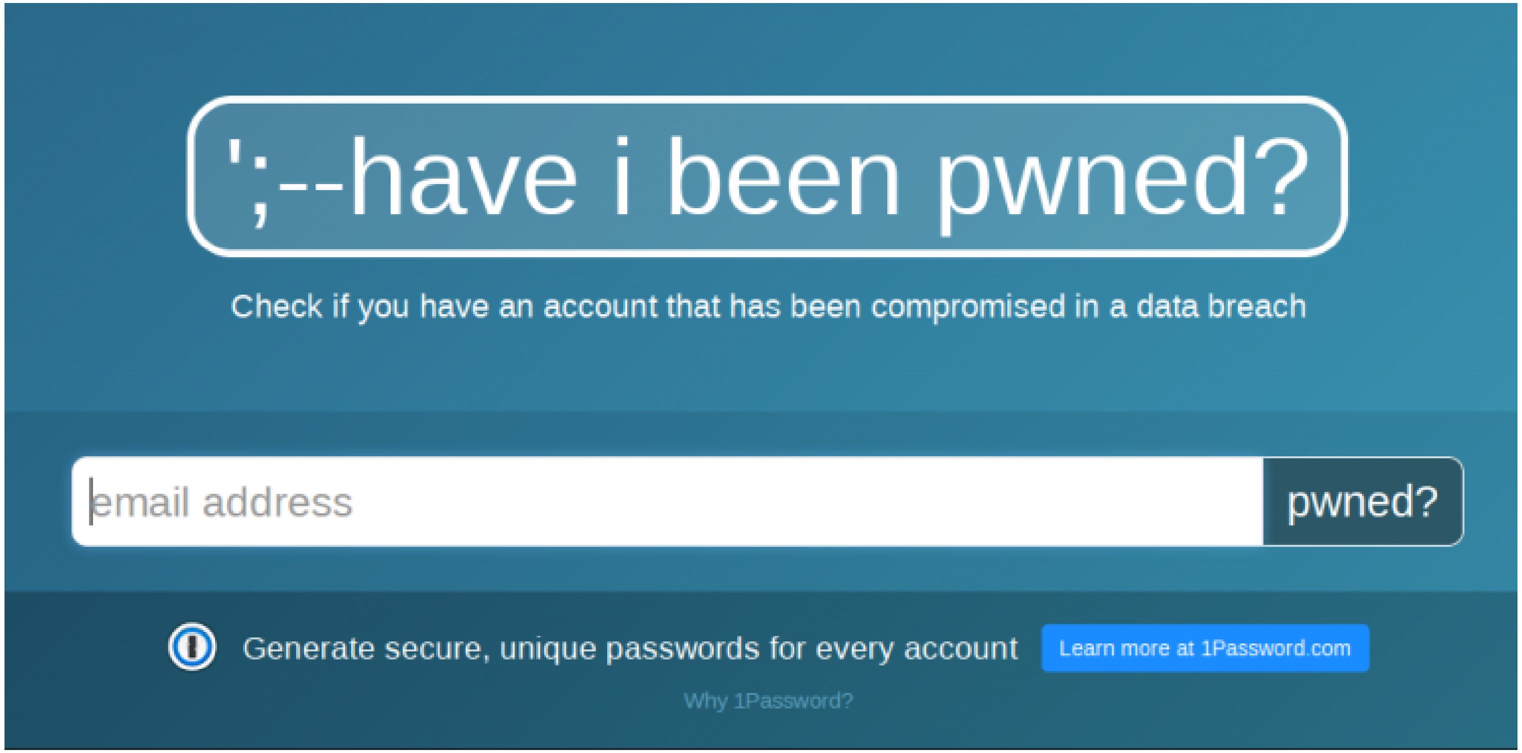


Personal	name, age, dob, phone, email, address, ip address, vehicle, height, parents, password
Employer	website/domain, email, phone, ip address, isp, mx, mail, ns1, port, job title, department nam

Earlier this year Jake Creps posted an interesting piece of research on how to locate Pastebin pastes that are unlisted and don't show up in Google searches. I recommend you read Jake's article in full, but by using the following Google search it would be possible to search for an e-mail in a Pastebin dump listed on a site (such as a hacking forum) that either wasn't indexed by Google or was so far down the list of search results that it wasn't visible:

Intext:"pastebin.com" AND target@domain.com –inurl:"pastebin.com"

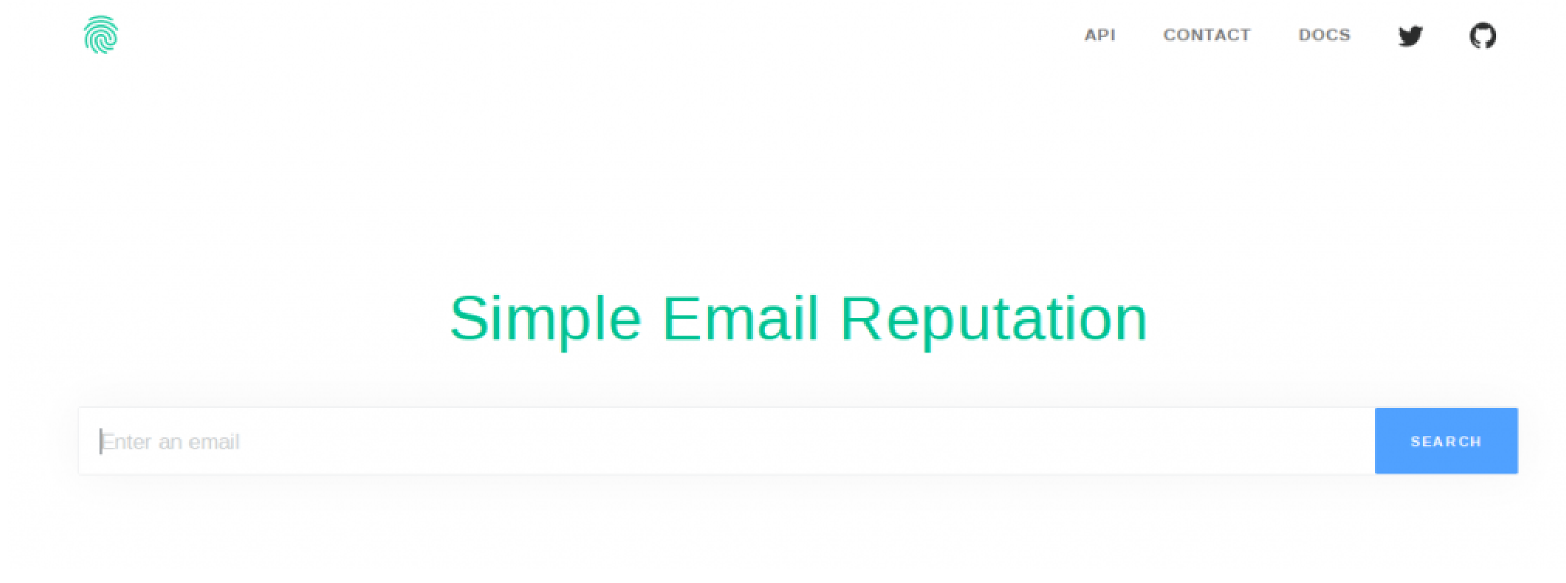
4. HaveIBeenPwned


';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?

HaveIBeenPwned is a well-known resource for checking if an e-mail has been involved in a data breach, but it can also be of use for OSINT purposes. When you find an e-mail that's been in a breach, HIBP will also show which data breaches it's been in. This will give some idea as to how old an e-mail address is, but more importantly it'll give you an idea as to which sites and services the target has (or had) accounts for. HIBP holds breaches for MyFitnessPal, Myspace, AdultFriendFinder, Ancestry, Snapchat, and many, many others. Identifying the breaches your target's e-mail has been in allows you to identify which sites or services they have used and begin working from there, perhaps with the username technique mentioned in point #2 above.

H8Mail is also a great command-line tool for identifying breached e-mails. Dehashed offers a similar paid-for service that includes the passwords as well as the e-mail addresses, but a note of caution here: whichever country you live in, it's almost certain that obtaining someone's password and accessing their e-mail without their authorisation is a criminal offence. It's certainly far beyond the scope of what can properly be called OSINT.

5.Emailrep.io



Emailrep.io is a great service designed to identify the age of an e-mail account, whether or not it's linked to phishing, and which other social media accounts it is known to be associated to. This is useful for those dealing with phishing and spammers, but it's also handyas an OSINT tool. I've tried it with several e-mail addresses and it has successfully identified a number of social media services associated to those e-mails, but just be aware that it by no means capture all of them. To check an e-mail, use the following URL:

https://emailrep.io/target@domain.com

You can also query the API directly from the command line with the curl command:

```
curl emailrep.io/target@domain.com
```

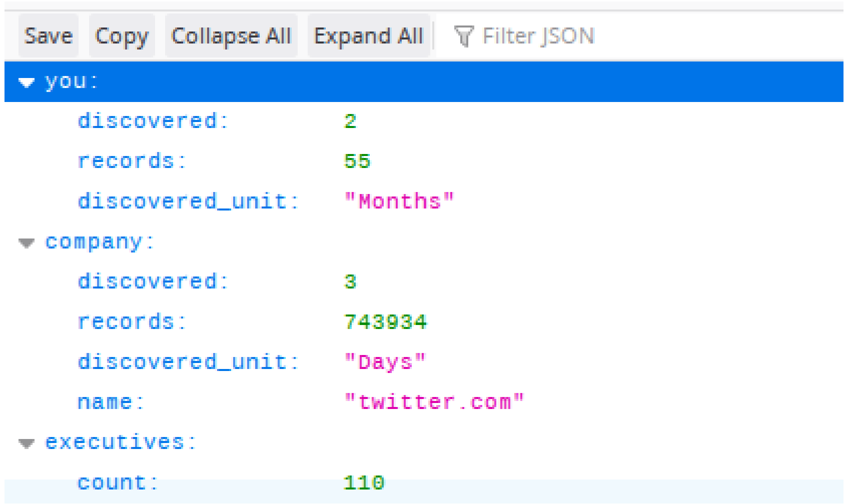
Both methods produce a JSON file containing a lot of useful information. Here’s an example for the e-mail address jack@twitter.com:

```
$ curl emailrep.io/jack@twitter.com
{
  "email": "jack@twitter.com",
  "reputation": "high",
  "suspicious": false,
  "references": 25,
  "details": {
    "blacklisted": false,
    "malicious_activity": false,
    "malicious_activity_recent": false,
    "credentials_leaked": true,
    "credentials_leaked_recent": false,
    "data_breach": true,
  "first_seen": "07/01/2008",
  "last_seen": "02/25/2019",
  "domain_exists": true,
  "domain_reputation": "high",
  "new_domain": false,
  "days_since_domain_creation": 7179,
  "suspicious_tld": false,
  "spam": false,
  "free_provider": false,
  "disposable": false,
  "deliverable": true,
  "accept_all": true,
  "valid_mx": true,
  "spoofable": false,
  "spf_strict": true,
  "dmarc_enforced": true,
  "profiles": [
    "foursquare",
    "pinterest",
    "facebook",
    "linkedin",
    "twitter",
    "spotify",
    "gravatar"
  ]
}
```

Pretty useful eh?

Spycloud has a similar tool, but it returns a much smaller amount of data. The URL to search with is:

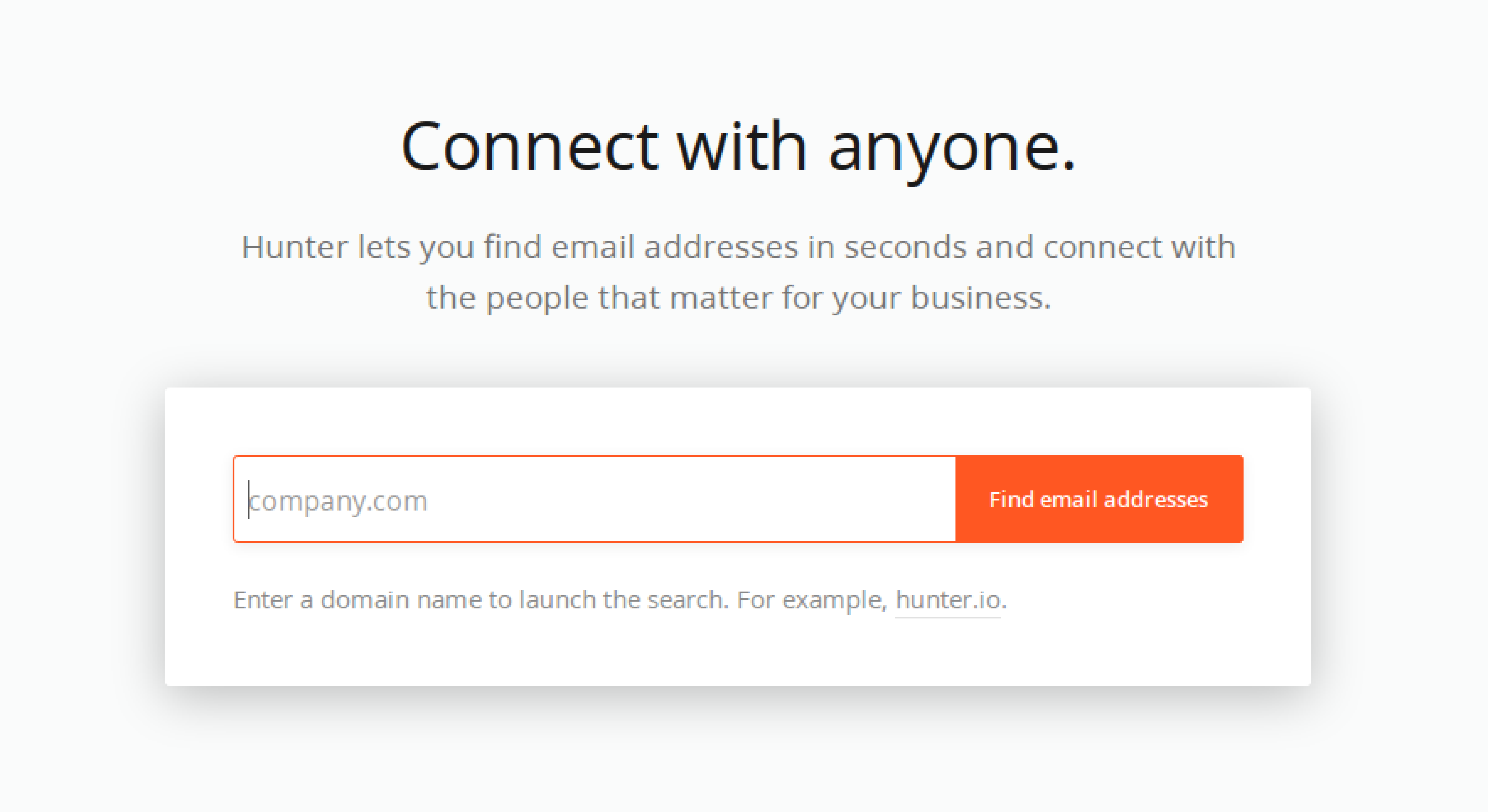
https://portal.spycloud.com/endpoint/enriched-stats/user@email.com



```
▾ you:
    discovered:       2
    records:          55
    discovered_unit:  "Months"
▾ company:
    discovered:       3
    records:          743934
    discovered_unit:  "Days"
    name:             "twitter.com"
▾ executives:
    count:            110
```

The above image shows the results for a query into **jack@twitter.com**. As you can see it returns much less information than Emailrep.

6. Hunter.io

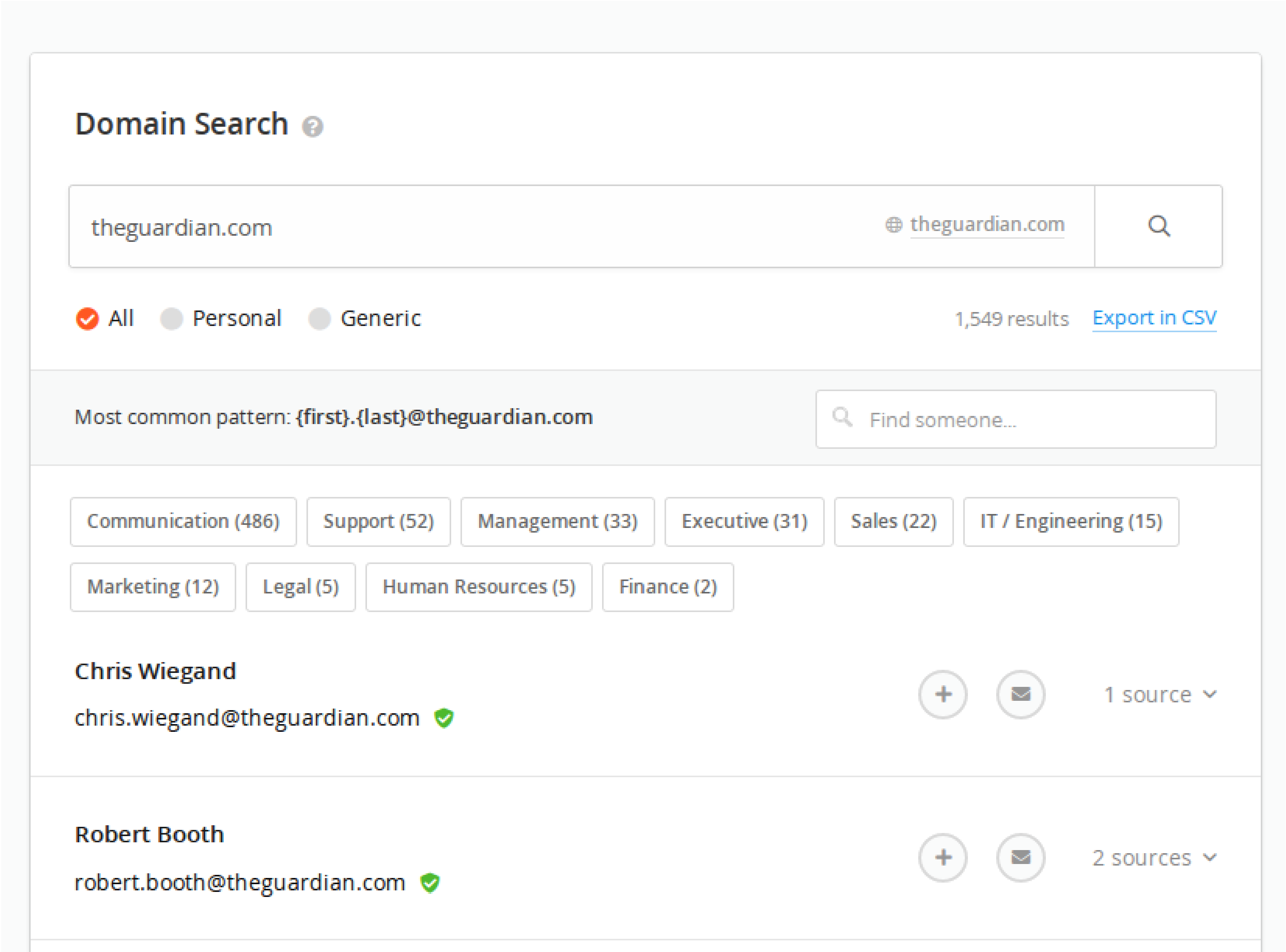


Connect with anyone.

Hunter lets you find email addresses in seconds and connect with the people that matter for your business.

Enter a domain name to launch the search. For example, hunter.io.

Hunter is an awesome e-mail OSINT tool. It's aimed at sales and recruitment professionals but that makes it great for OSINT too (you'll need to register though). It doesn't work with common e-mail providers like Gmail, but where an e-mail address is linked to an organisation's own domain then Hunter is extremely useful. In this example I'll use Hunter to look at e-mail addresses linked to the domain of the Guardian newspaper, theguardian.com.



Domain Search

theguardian.com

theguardian.com

● All ○ Personal ○ Generic

1,549 results Export in CSV

Most common pattern: **{first}.{last}@theguardian.com**

Find someone...

Communication (486) | Support (52) | Management (33) | Executive (31) | Sales (22) | IT / Engineering (15) | Marketing (12) | Legal (5) | Human Resources (5) | Finance (2)

Chris Wiegand

chris.wiegand@theguardian.com ✓

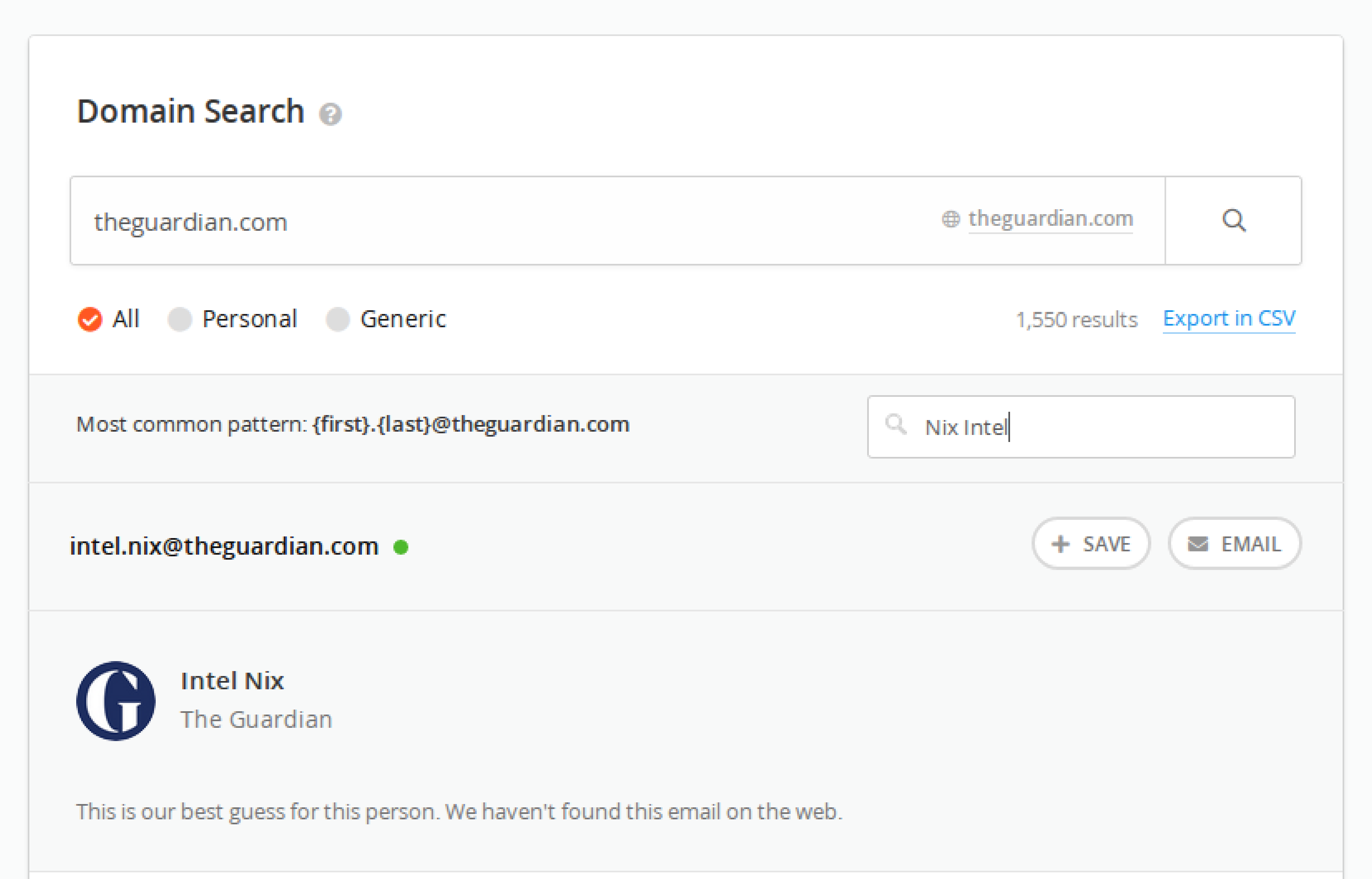
1 source

Robert Booth

robert.booth@theguardian.com ✓

2 sources

Hunter brings back a list of all the e-mail addresses that it has identified as being linked to that domain, and it's smart enough to identify which sector of the organisation they most likely work in. It also references the URL where the data was scraped from, which allows you to expand your search further by selecting the “sources” dropdown option on the right hand side. The URLs also stay referenced, even if the original page has been deleted.



Domain Search

theguardian.com

theguardian.com

● All ○ Personal ○ Generic

1,550 results Export in CSV

Most common pattern: {first}.{last}@theguardian.com

Nix Intel

intel.nix@theguardian.com ●

+ SAVE

EMAIL

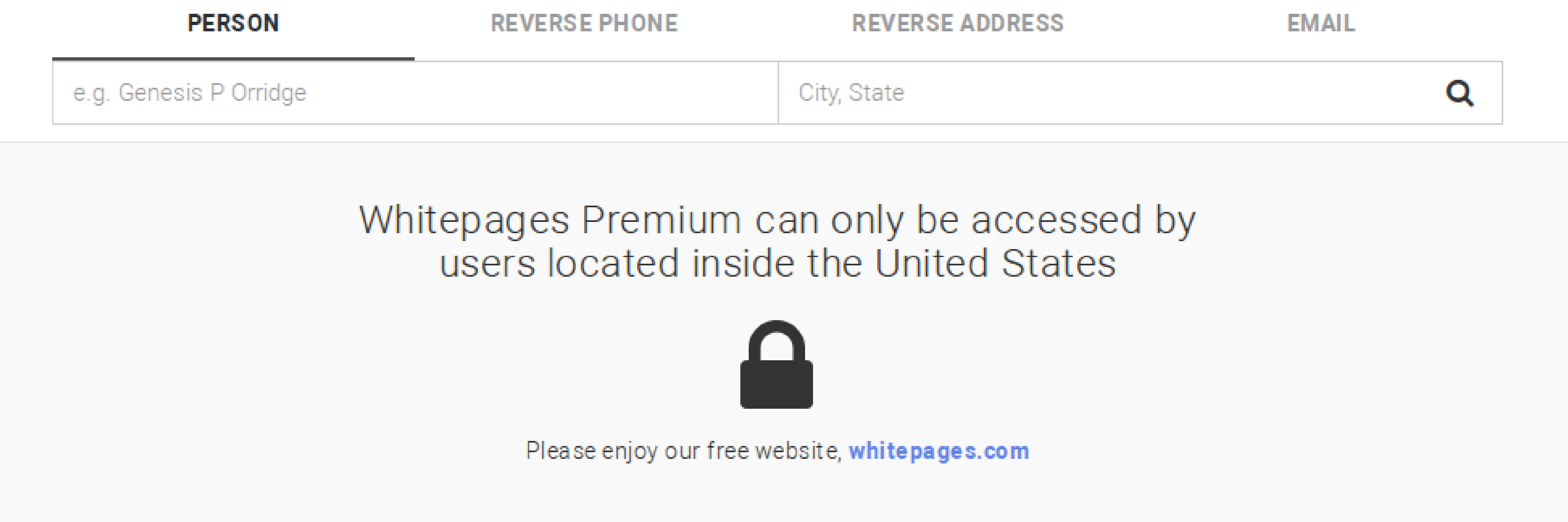
Intel Nix

The Guardian

This is our best guess for this person. We haven't found this email on the web.

Another useful feature is the ability of Hunter to predict the e-mail address of someone who works at that organisation, based on the format of email addresses it has already discovered. For example if I wanted to check if The Guardian employed someone called “Nix Intel”, I could enter the name into Hunter to predict the likely e-mail address. Even if it doesn’t find any matches, learning the e-mail format allows you to construct possible e-mails and try to find matches on other platforms like LinkedIn (see below).

7. WhitePages



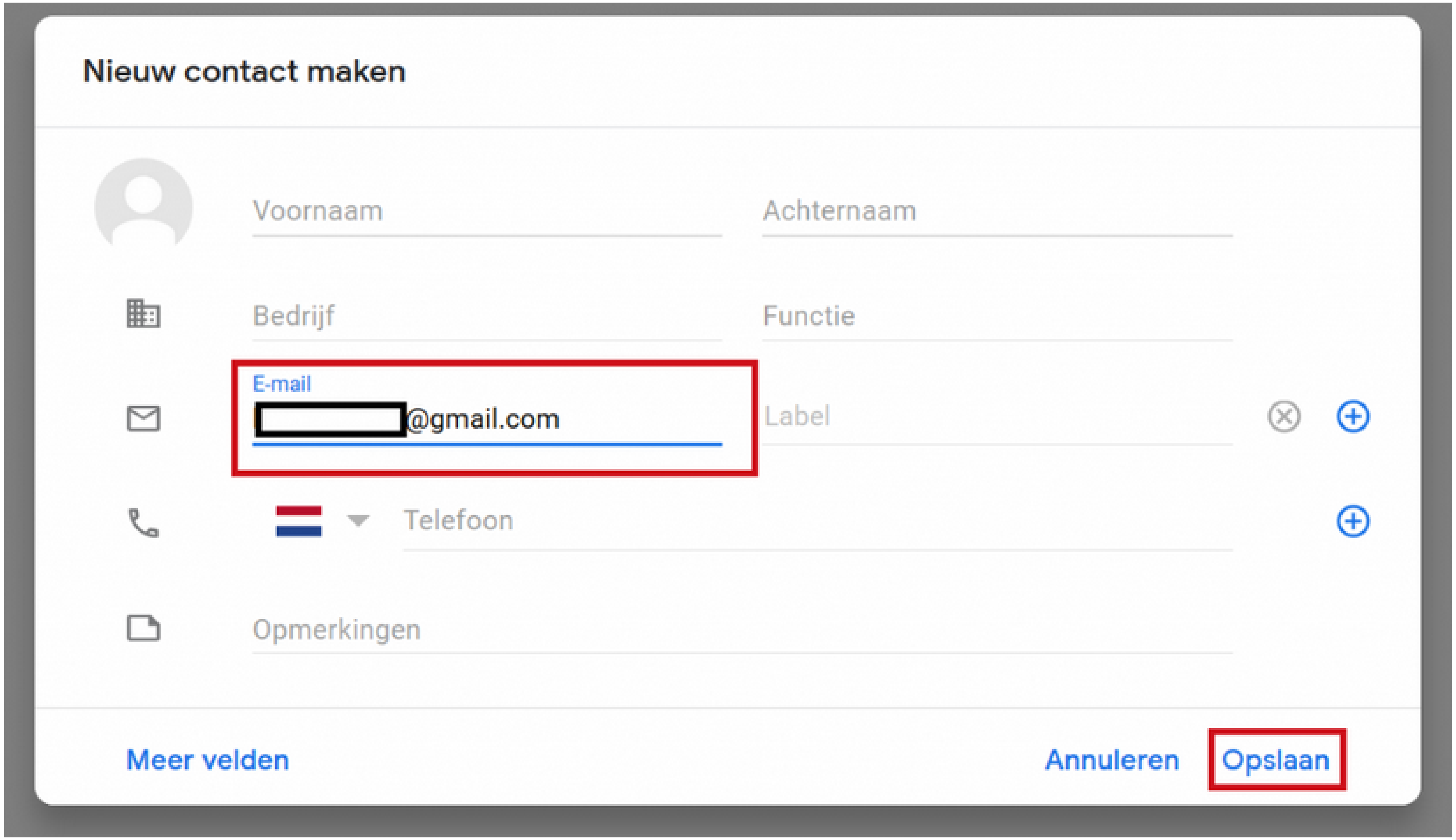
Whitepages Premium can only be accessed by users located inside the United States

Please enjoy our free website, whitepages.com

**Or by users located on the other end of a US VPN endpoint.*

WhitePages and similar services are useful for reverse e-mail lookups. These companies sit on a vast pile of data from hundreds of sources and can help link e-mails to other identifiers like addresses and phone numbers. However WhitePages is only worth paying for if you’re researching subjects in the US. Data protection and privacy laws mean that it isn’t possible for there to be a UK or EU equivalent to WhitePages, so it’s of limited value as an e-mail lookup tool if your subject resides in the EU.

8. Twitter – Gmail Sync



Nieuw contact maken

E-mail
[redacted]@gmail.com

Using the contact sync feature on some apps and services allows you to use an e-mail address to identify a subject's other social media profiles. Aware-Online researched and wrote a great article on this which I recommend you go and read in full. The technique involves creating a ghost Gmail profile and also a Twitter profile linked to the same account. Simply add your target e-mail as a

Gmail contact, let Twitter sync with your Gmail contacts and hey presto – if your target e-mail has a Twitter account associated to it then you'll be able to see it.

9. LinkedIn

LinkedIn is full of OSINT opportunities, including for e-mail research. LinkedIn allows you to tweak a URL to see if there is a profile linked to any given e-mail account. The URL is as follows:

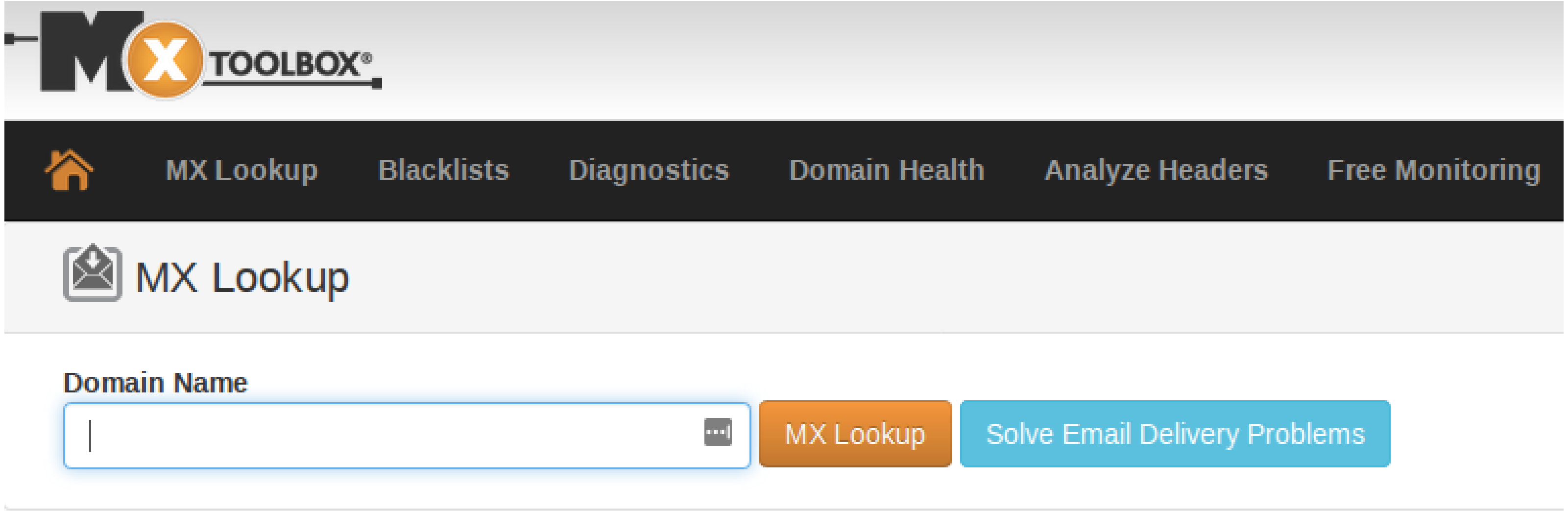
https://www.linkedin.com/sales/gmail/profile/viewByEmail/user@domain.com

If there is a LinkedIn account associated to the e-mail, it'll be displayed.

Osint.support now also has a browser add-on available to automatically match LinkedIn accounts to e-mail addresses, and there's also a web portal to do this at ThumbTube.

But what if you want to work the other way round from a LinkedIn Profile to an e-mail? Matthias Wilson did some excellent research into this topic and really you should read his full post here. In a similar way to the Twitter method mentioned above, Matthias used the way in which Gmail syncs with other services to try to find the e-mail address of someone he found on LinkedIn. He knew their name, and so he used E-mail Permutator to generate a list of probable e-mail addresses. Entering all these into Gmail and then seeing which addresses sync with a LinkedIn profile helps to identify the person's e-mail address, even if you don't know it at the outset.

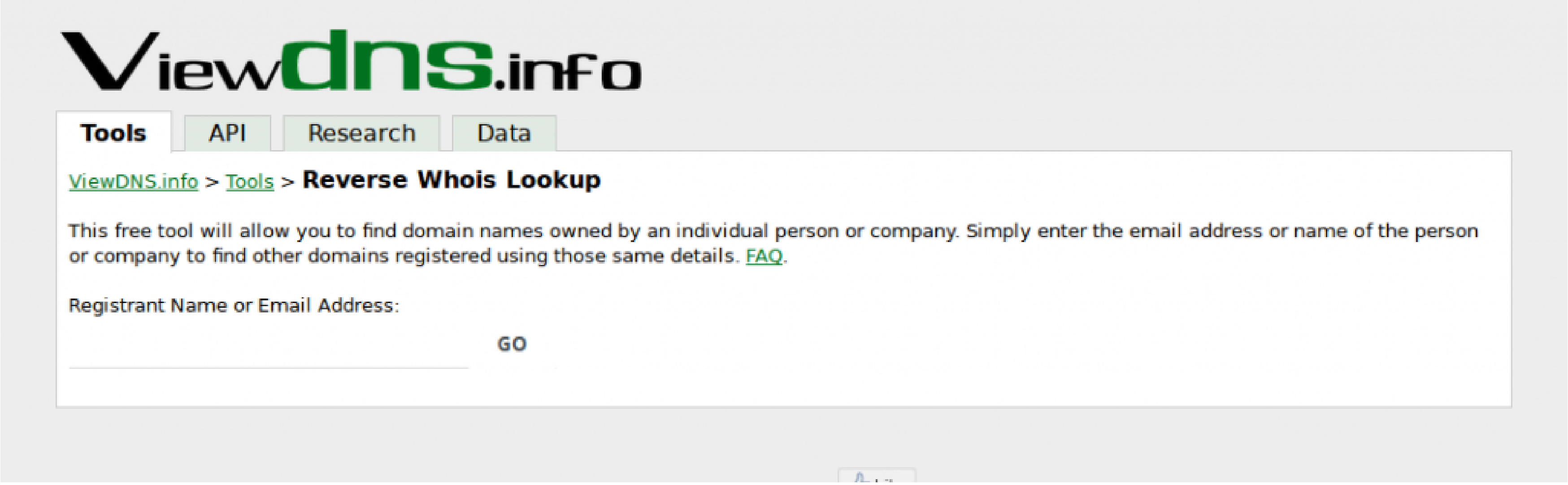
10. MxToolbox



MxToolbox is a long-established service for diagnostics and lookups for MX (mail exchange) servers. It isn't so useful for e-mails from popular e-mail domains like Gmail, but where a subject uses an e-mail service with its own mail exchange server (which most large organisations typically do), MxToolbox can help. Identifying a mail exchange server IP address can be a good starting point to move on and look at shared IP addresses, nameservers, reverse IP and other network architecture in order to learn more about your subject's organisation and web presence. I wrote a previous blog post about that here and here, but an MX server can be a great starting point for these kind of OSINT enquiries.

MxToolbox also offers an e-mail header analysis service. The limitation of this is that you need to be in possession of an e-mail directly from your subject, since the header is overwritten if an e-mail is sent on elsewhere. If you do have an e-mail header (find out how to obtain one here), MxToolbox is able to identify the originating IP address, amongst other things. There is a limitation to this though – the increasing prevalence of cloud-based e-mail services like Office365 means that the originating IP address is much more likely to come from a cloud service provider, and not a location linked directly to the subject.

11. WhoIs



ViewDNS.info > Tools > **Reverse Whois Lookup**

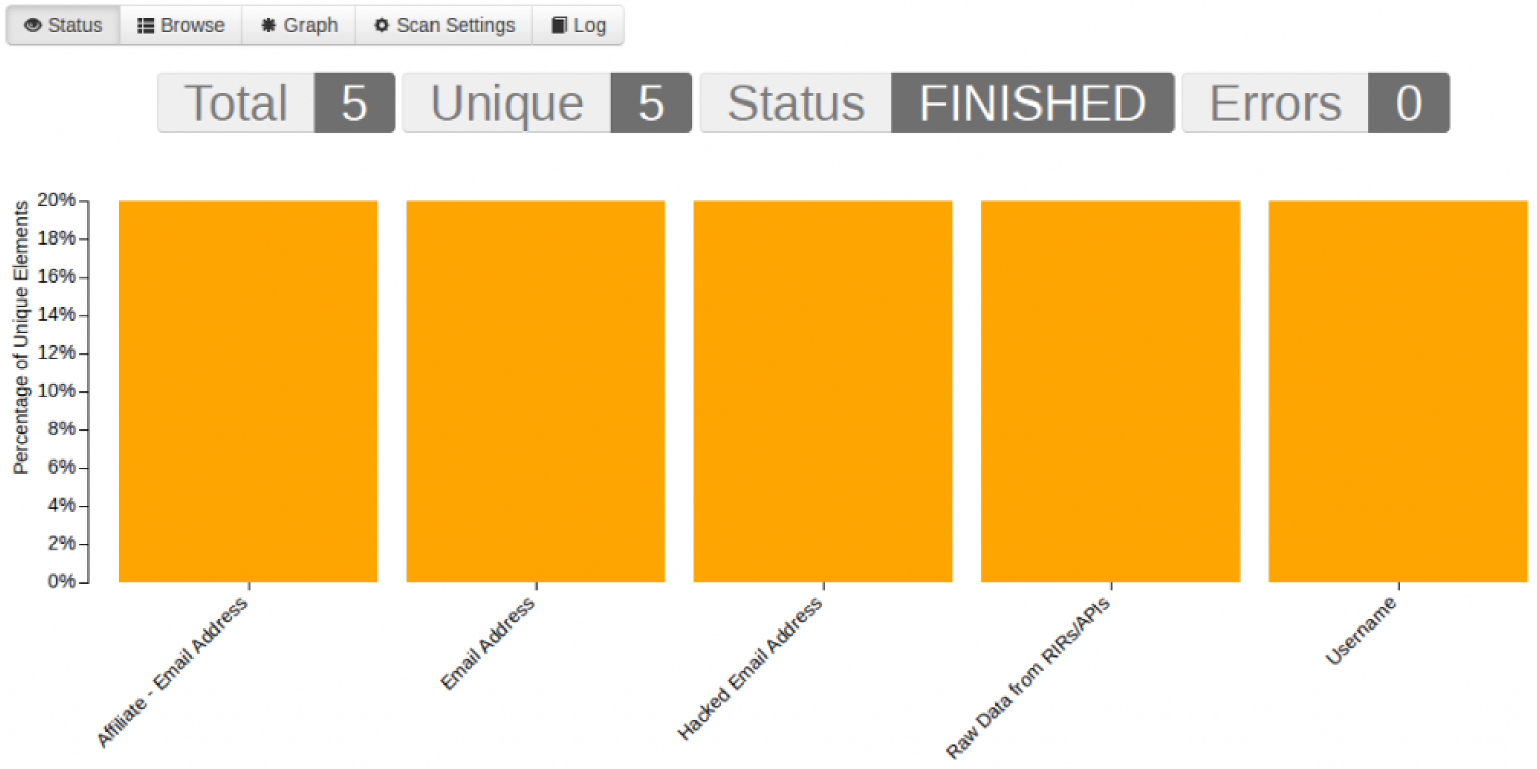
This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

There's no doubt that WhoIs is much less useful as an OSINT than it once was due to the rise of anonymising services and legislation like GDPR. However there are still plenty of e-mail addresses linked to WhoIs domain and IP records, either as registrants, tech support, or even abuse contacts. There are a few tools that can search WhoIs records, but ViewDNS have a nice simple interface for checking e-mails against registrant information here.

12. Spiderfoot



Total 5 Unique 5 Status FINISHED Errors 0

Spiderfoot is a fantastic tool for automating OSINT queries. Explaining how to set up and run Spiderfoot would be a separate blog post altogether (coming soon…) but it's a well-supported tool with great documentation. There are dozens of different search modules available but there are a few specific to e-mail addresses that you'll want to enable. Some of these are:

BotScout	Searches botscout.com's database of spam-bot IPs and e-mail addresses.
E-Mail	Identify e-mail addresses in any obtained data.

EmailFormat	Look up e-mail addresses on email-format.com.
BuiltWith	Query BuiltWith.com's Domain API for information about your target's web technology stack, e-mail addresses and more.
Clearbit	Check for names, addresses, domains and more based on lookups of e-mail addresses on clearbit.com.
IntelligenceX	Obtain information from IntelligenceX about identified IP addresses, domains, e-mail addresses and phone numbers.

There are plenty of others, including some modules that will automate checks with HaveIBeenPwned and Hunter.io that I've desrcibed above.

Simply give your search a title, enter the e-mail address you're searching for, make sure the relevant modules are enabled, and let Spiderfoot crawl away to find some results.

Are there any other good e-mail tools and techniques that I've missed? Let me know on Twitter if there's some others that I should include.

domains, E-mail, H8mail, OSINT, OSINT Tools, resources, Sherlock, Techniques, Tools, Tutorials & Guides, website attribution

← One Search To Rule Them All – Boolean Searches For Images

Where In The World? Global and Local Identifiers – Quiztime 12th Sept 2019 →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Search …

Search

Recent Posts

Gap Analysis: Chrono and Geolocation In Berlin (Quiztime 7th October 2019)

Digital Shadows: Seeking Sector035 – Quiztime 26th September 2019

Search Tip: Finding Historic WhoIs Data

Getting Started With Spiderfoot – A Beginner’s Guide

The Attrition of Information in OSINT: Why Acting Quickly Matters, And How To Recover When You Don’t.

Recent Comments

altitude training on Quiztime 25th August 2019 – Military Vehicles & Geolocation

An OSINT guide for military research – Center for Undersøgende Journalistik on Quiztime 25th August 2019 – Military Vehicles & Geolocation

Stefan (@dersteff) on Quiztime 25th August 2019 – Military Vehicles & Geolocation

@dersteff on Quiztime 25th August 2019 – Military Vehicles & Geolocation

Stefan on Two Different Approaches To Photo-Geolocation

Tags

- 8chan
- aircraft
- Bellingcat
- Cloudflare
- Digital Forensics
- DIY Buscador
- domains
- Facebook
- financial
- fingerprinting
- Gasmask
- geolocation
- government
- H8mail
- images
- Instagram
- InstagramOSINT
- Investigation
- Kik
- Linux
- Live OSINT
- OneMillionTweetMap
- opsec
- OSINT
- OSINT Tools
- Phoneinfoga
- Photon
- privacy
- Python
- Quiztime
- resources
- reverse ip
- Sherlock
- Snapchat
- Techniques
- theHarvester
- Tools
- Training
- Treeverse
- Tutorials & Guides
- Twitter
- usernames
- website attribution
- whois
- YouTube

Categories

- Linux
- OSINT
- OSINT Tools

Archives

- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019

Blog Kit by WP Charms