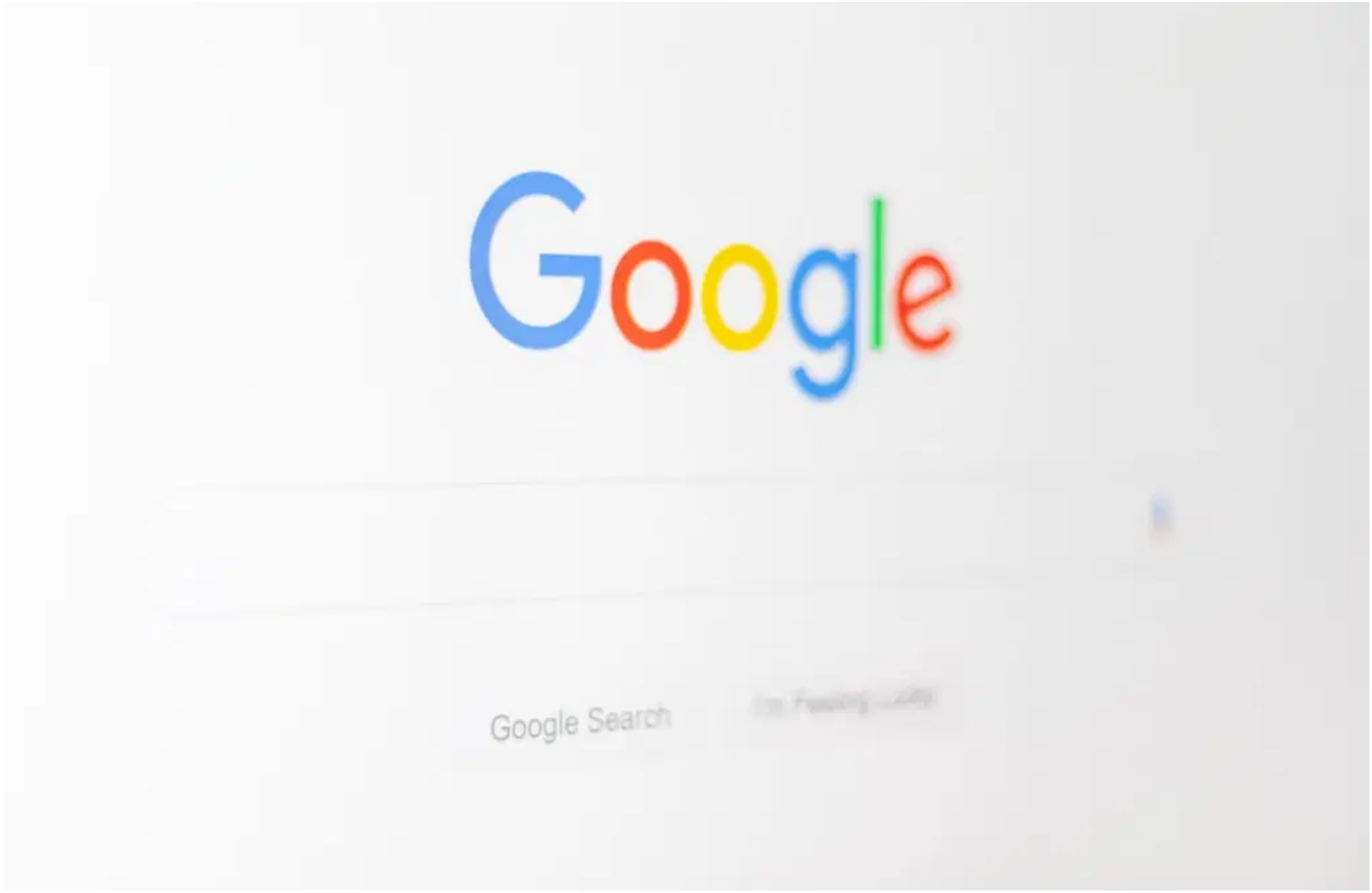
We are OSINTCurio.us



OSINT

Google Dorks

The term ‘Google dorks’ has been around for quite some years by now and is used for specific search queries that use Google’s search operators, combined with targeted parameters to find specific information. And in the webcast/podcast of early December we reached out to the listeners, to send us your favourite Google Dork.

We grouped the dorks by the type of target information that it is used for, starting with the human being:

People and Accounts

The first one that was posted on Twitter after we talked about it, came from **Kirby**. She loves to find emails based on a username, so she lets Google do the heavy lifting. Instead of searching for all possible email providers, she replaced the domain name with an asterisk:

```
"username*com"
```

OSINT Techniques shared his favourite dork, that searches for online resumes of a person. You can search within the URL of a website, or within the text of a site:

```
inurl:resume “john smith”
intext:resume “john smith”
```

OSINT Combine also shared a tweet that focuses on jobs. By targeting the LinkedIn site, he searches for people with a specific job title and location. But he shared another trick, which is the fact that you can search for icons or Unicode characters:

```
site:http://linkedin.com/in "<job title>" (☎ OR ☏ OR ✆ OR 📱
```

And in case you are looking for a specific name, you can of course always search for:

```
"<name>" (☎ OR ☏ OR ✆ OR 📱)
```

The last dork touching people that was sent to us via Twitter, came from **Jung Kim**. He shows a nice dork to find people within GitHub code:

```
site:http://github.com/orgs/*/people
```

And if you are looking for lists of attendees, or finalists, **Jung Kim** shared a second dork with us:

```
intitle:final.attendee.list OR inurl:final.attendee.list
```

Another tips was given by **Nixintel**, that searches for login information on a Trello board. Since a lot of people forget to tighten the security

settings on their Trello board, loads of them are exposed and indexed by Google:

```
site:http://trello.com password + admin OR username
```

Documents

To finding specific documents within a website or domain name, **CyberSquarePeg** shared with us the basic Google dork to do just that:

```
site:<domain> filetype:PDF
```

Note: Instead of 'filetype:' you can also use the abbreviation for extention, which is: 'ext:'

Alex shared with us a search that is also targeting PDF's, but he shows how to search for only those documents that might contain possible email information. Change the <domain> to the specific company domain name and have a look what's out there:

```
filetype:pdf <domain> "email"
```

Zerconil shared a dork that is looking for XLS files within government websites:

```
filetype:xls site:.gov
```

Of course you can look for more extensions, depending on what you are trying to achieve. You do that by adding multiple file extensions in between double quotes, where each of the extensions is being separated by a pipe of vertical line '|'. And don't forget to add extra spaces around it:

```
filetype:"xls | xlsx | doc | docx | txt | pdf" site:.gov
```

In case you are looking for even more extensions that might be of interest, Twitter user **Insider** helped us out there with his tip that he

sent via Twitter:

```
filetype:"doc | pdf | xls | txt | ps | rtf | odt | sxw | psw |
```

And another tip shared by **Jung Kim**, this time searching for any kind of document on HubSpot that contains the word ‘trends’ and that has the year 2019 in the URL:

```
site:http://cdn2.hubspot.net intitle:2019 OR inurl:2019 "* tre
```

Dutch_Osintguy shared another one targeting Google as email platform with looking for txt OR pdf files containing words like FBI, CIA Or NYpD (these are interchangeable by words by your particular interest):

```
"Email delivery powered by Google" ext:pdf OR ext:txt nypd OR
```

Cloud, Buckets and Databases

Dutch_OsintGuy shared one of his favorite dorks. This one is searching for indexed documents that contain the phrase ‘confidential’ or ‘top secret’ within open Amazon S3 buckets:

```
site:http://s3.amazonaws.com confidential OR "top secret"
```

Another search touching Amazon buckets came from **Zerconil**, that might show some confidential login information within XLS files:

```
s3 site:http://amazonaws.com filetype:xls password
```

And here again the tip of maybe adding all kinds of interesting extensions, since Excel files might not be the only interesting document format that contain the information you are looking for.

And of course you can search for copies of databases via Google too. To find some of them, simply search for:

```
ext:sql intext:"-- phpMyAdmin SQL Dump"
```

Social Media

Jules Darmanin shared a tip on how to find out whether a certain tweet was shared on other media, for instance a news site. For that, search for the specific text and tell Google to ignore anything that was posted within twitter.com by adding the minus sign to that part of the dork:

```
"text of a tweet" -site:https://twitter.com
```

Almost the same method can be used to search messages and/or links for a specific username not coming from that username his/her account. For example this searches for links or information containing '@dutch_osintguy' but not coming directly of the twitter user timeline Dutch_osintguy

```
@dutch_osintguy -site:twitter.com/dutch_osintguy
```

Want to learn more about Google Dorking ?

Using Google search operators as effective as possible is an art by itself. For OSINT the goal is (most of the time) to create your targeted haystack. But by using **well chosen keywords** and dorked together with **the right search operators** you will be able to create a haystack with as **low** a possible **volume** with an as **high** as possible **probability**.

Keep in mind that Google has limited the amount of keywords that you can search for to a total of 32 words. This means that all search term beyond the 32 word limit will not be taken into account (keyword 33 and beyond) in a search. Also there is a character limit per one keyword. A single keyword can not be longer than 2048 characters.

All of the above Google dorks came from a specific intelligence requirement question. Without a good question it is way harder to craft your search query is targeted as possible. So an advice might be, what are you looking for? What question are you trying to answer? That makes it easier to pinpoint which search operators might be needed to answer that specific question.

For extra inspiration you might want to look into sources like the **Google Hacking Database**. This is a website that collects user generated Google dorks with a specific need or interest. Another great resource to learn how to craft a good Google dork is the **GoogleGuide**. The GoogleGuide is a good website to see which Google search operators are available and how you can use them for your research. Even though it is a bit old (info from 2007) the GoogleGuide still has a lot to offer en learn from when you are OSINTcurious. Another option is the **ahrefs blog** about Google search operators. They visually explain how you an use 42 search operators.

There is also one Google Dorking book which is a must read when it comes to learning and understanding how to use google searches for research. It is a book by **Johnny Long** with the title "**Google hacking for penetration testers**". Within the osint community there is a debate on which version is the best for OSINT practitioners. My personal (Dutch_Osintguy) opinion is that version 1 of this book is the best and most complete. Non the less all other versions (there are 3 editions) are worth the read.

This blog was made by: **@sector035 @dutch_osintguy** & **@technisette**

P.S. Liked this post? Sponsor The OSINT Curious Project via **Patreon** for as little as $1 per month 🙂 Thanks!

SECTOR035

2019-12-20

#BOLEAN SEARCHING, #GOOGLE DORKS, #GOOGLE HACKING, #GOOGLE HACKS, #GOOGLE X-RAY, #SEARCH OPERATORS, #SOURCING

SHARE THIS:

LIKE THIS:

Like

Be the first to like this.

4 thoughts on “Google Dorks”

Jung Kim (@Azn_CyberSleuth)

2019-12-20 AT 06:03

Fantastic!

★ Like

REPLY

Pingback: **Infosec Reading List – December 2019 | Dominik Birk**

Pingback: **Google Dorks | digithek blog**

Pingback: **START CARING STOP SHARING Stories by Dutch Osint Guy on Medium – DeFi News**

Leave a Reply

Enter your comment here...

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

PREVIOUS
Our merch store!

NEXT
Introduction to OSINT Video

Creative Commons License