What is Google Dorking?

- Google Dorking is a search technique that enables hackers to gain access to information that corporations and individuals did not intend to make publicly available.
- Using this technique, hackers are able to identify vulnerable systems and can recover usernames, passwords, email addresses, and even credit card details. Used effectively, Google Dorking is a valuable hacking shortcut to finding systems and data of interest.
- Google Dorking is unusual in that it is not a hack, vulnerability, or an exploit, hackers are just making use of publicly available advanced search tools. It isn't new either; attackers have been making excellent use of search provider data to gather intelligence on targets and find vulnerable systems for years.
- In fact, there are a number of websites and communities dedicated to the use and study of Google Dorking, many with example searches that date back more than 10 years.
- The most concerning thing about Google Dorking is the sheer volume of online information that can help the uninitiated and skilled alike.
- Some of the resources are educational, some are nefarious. Either way, these resources put an astonishing amount of capability in the hands of anyone that is interested.

How does Google Dorking work?

- Search engines crawl the Internet and index page titles, link data, and page contents, and store the data in a way that is optimal for satisfying search queries. Unfortunately, the crawlers also index other material they find, even if developers, administrators, and website owners did not intend it to be public.
- Malicious actors can craft queries that will find interesting or useful clues from this information, such as:
  - Exposed critical directories
  - Vulnerable files and servers
  - Files containing usernames and passwords
  - Sensitive online shopping info

Special google search operators

intitle:

This will ask google to show pages that have the term in their html title.

inurl:

Searches for specified term in the URL. For example: inurl:register.php

filetype:

Searched for certain file type. Example: filetype:pdf will search for all the pdf files in the websites.

ext:

It works similar to filetype. Example: ext:pdf finds pdf extension files.

intext:

This will search content of the page. This works somewhat like plain google search

site:

This limits the search to a specific site only. Example: site:abc@d.com will limit search to only abc@d.com.

Cache:

This will show you cached version of any website. Example: cache: aa.com

*

This works like a wildcard. Example: How to * sites, will show you all the results like “how to…” design/create/hack, etc… “sites”

How can we be Safe?

There are a number of ways to mitigate Google Dorking, mostly enforcing enforce system best practices and improving granularity of access control:

- Keep Operating Systems, services and applications patched and up-to-date.
- Make use of security solutions that prevent intrusion and data egress.
- Understand how search engine crawlers work, know what is public, and audit your exposure.
- Move sensitive resources out of public locations.
- Block access to all non-essential resources from external or foreign identities.
- Perform frequent penetration testing.

References

https://www.mcafee.com/blogs/enterprise/google-dorking/

https://medium.com/infosec/exploring-google-hacking-techniques-using-google-dork-6df5d79796cf

https://www.simplilearn.com/tutorials/cyber-security-tutorial/google-dorking