DEFINITION

Google dork query

Rahul Awati

Ivy Wigmore

What is a Google dork query?

A Google dork query, sometimes just referred to as a *dork*, is a search string or custom query that uses advanced search operators to find information not readily available on a website.

Google dorking, also known as *Google hacking*, can return information difficult to locate through simple search queries. This includes information not intended for public viewing, but that is inadequately protected and can, therefore, be "dorked" by a hacker.

How Google dorking works

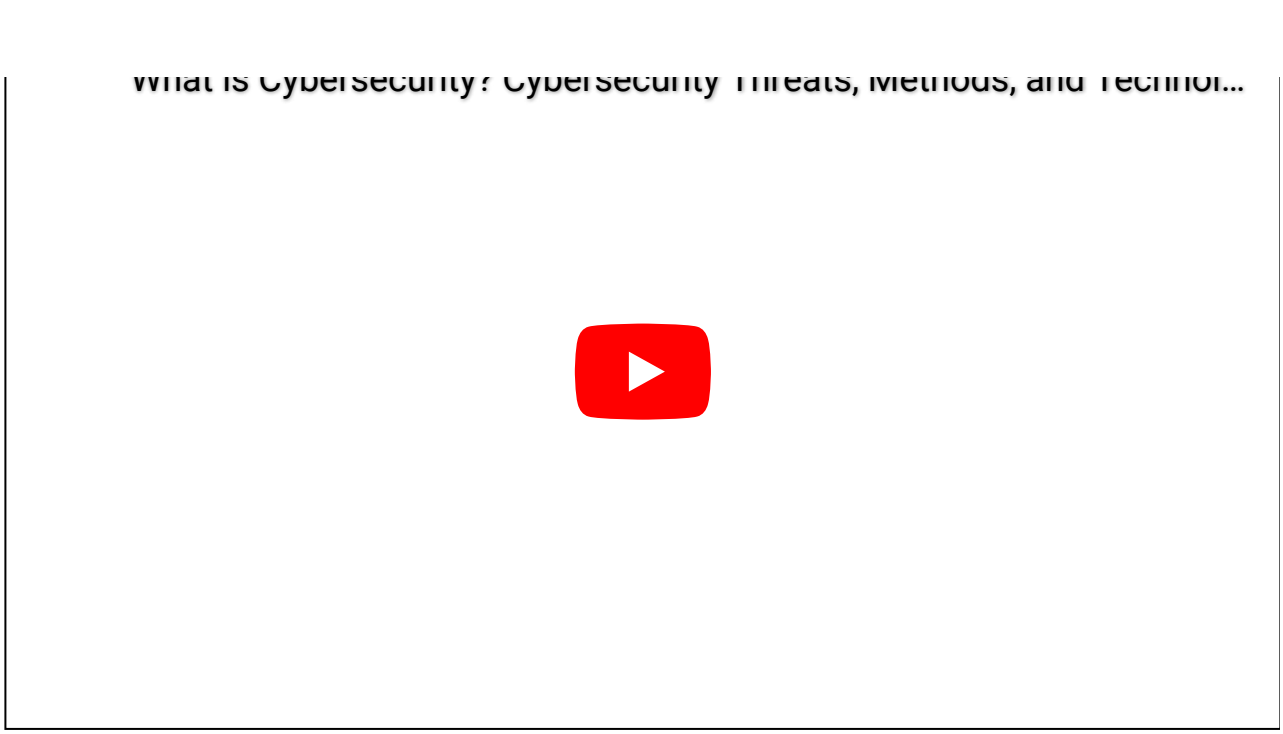
Google dorking is a passive attack or hacking method involving the use of a custom query. Hackers use Google to identify websites with security vulnerabilities and/or sensitive information the attacker can use, usually for some malicious purpose.

Around since 2002, dorking usually involves using a search engine as a hacking tool. Google's tremendous web crawling capabilities facilitate dorking. With a Google dork, attackers can access a lot of information they wouldn't be able to get with simple queries. This information includes the following:

- usernames and passwords
- email address lists
- sensitive documents
- personally identifiable information
- personally identifiable financial information
- website vulnerabilities

More often than not, this information is used for many types of illegal activities, including cybercrime, cyberterrorism, industrial espionage, identity theft and cyberstalking. Hackers may also sell this data to other criminals on the dark web for large sums of money

What is Cybersecurity? Cybersecurity Threats, Methods, and Technol



In August 2014, the United States Department of Homeland Security, Federal Bureau of Investigation and National Counterterrorism Center issued a bulletin, warning agencies to guard against Google dorking on their sites. Among the intrusion prevention measures proposed was to conduct Google dorking expeditions using likely attack parameters to discover what type of information an intruder could access.

9 key features of network security

Network security involves nine key features.

Metadata and Google dork queries

Multiple parameters can be used in a Google dork query to search for files or information on a website or domain. For the website, https://www.governmentwebsite.gov, this string returns PDF documents with "sensitive but unclassified" anywhere in the text:

"sensitive but unclassified" filetype:pdf site:governmentwebsite.gov

A hacker that gets access to internal documents on a website can potentially also get additional sensitive information. For example, document metadata often contains more information than the author may be aware of, such as name, revision history, deletions, dates, etc.

An intruder knowledgeable about Google dorking and armed with hacking tools can access sensitive information from metadata fairly easily. That's why it's a good practice to remove all metadata from documents before publishing them on a website. Document sanitization can also ensure that only authorized users can access the intended information.

Common Google dork operators

A search parameter in a Google dork is applied to a search on the search engine. Google has its own query language built in, and hackers use these queries to find sensitive files, track people and discover web vulnerabilities a simple search does not reveal.

Here are some popular search parameters often used in Google dorks.

Operator	Function	Example
cache:	Returns the cached version of a website	cache:techtarget.com
site:	Returns a list of all indexed URLs from a website or domain	site:techtarget.com
filetype:	Returns various kinds of files, depending on the file extension provided	filetype:pdf
inurl:	Searches for a specific term in the URL	inurl:register.php
allinurl:	Returns results whose URL contains all the specified characters	allinurl:clientarea
intext:	Locates webpages that contain certain characters or strings inside their text	intext:"Google Dork Query"
inanchor:	Searches for an exact anchor text used on any links	inanchor:"cyber attacks"

Operator	Function	Example
|	Shows all sites that contain either or both specified words in the query	hacking | Google dork
+	Concatenates words to detect pages using more than one specific key	hacking + Google dork
-	Used to avoid displaying results containing certain words	hacking - dork

Examples of Google dorks

Here are some ways attackers use Google dorks to extract sensitive information from websites via Google.

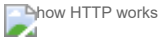
1. To extract log files

Many kinds of error logs, access logs and application log types are available in the public Hypertext Transfer Protocol (HTTP) space of websites. Attackers can use a Google dork to find these files and any information the site may contain about its PHP version, content management system paths, admin credentials, user credentials, etc.

Example search query

allintext:password filetype:log after:2010

To prevent hackers from using such dorks to access important logs, website owners and admins must properly configure the robots.txt file.



Hackers can use a Google dork to find error and access logs, as well as application logs publicly available in website HTTP spaces.

2. To open and exploit FTP servers

Google indexes both HTTP-based and open File Transfer Protocol servers, which enables attackers to explore public FTP servers. Weak access permissions on FTP servers can result in sensitive information getting published unintentionally.

Example search query

intitle: "index of" inurl:ftp

3. To find SSH private keys and decrypt information

Secure Shell private keys decrypt information exchanged in the SSH protocol. These keys should not be shared with anyone -- hence the term private. However, a hacker may use a Google dork to find and exploit the SSH private keys indexed by Google to decrypt and read sensitive information an authorized user would want to protect.

Example search query

intitle:index.of id_rsa -id_rsa.pub

4. To find HTTP websites

Attackers can use a Google dork to discover websites or forums using the less secure HTTP protocol.

Example search query

intitle:"index of" inurl:http after:2015

They can also search for websites or specific educational or governmental organizations with the .edu or .gov domain extensions using this query:

"inurl:."domain"/"dorks""

5. To hack into online cameras

Public closed-circuit television cameras are usually plugged in to the internet and are, therefore, a common target of hackers and cybercriminals. With Google dorking, hackers can fetch live camera webpages unrestricted by IP. Sometimes, they may also be able to control the admin panel remotely and even reconfigure the cameras.

Example search query

inurl:top.htm inurl:currenttime

Zoombombing has also become prevalent in the post-COVID-19 world. This is when a hacker disrupts a Zoom meeting using a Google dork query, like the following:

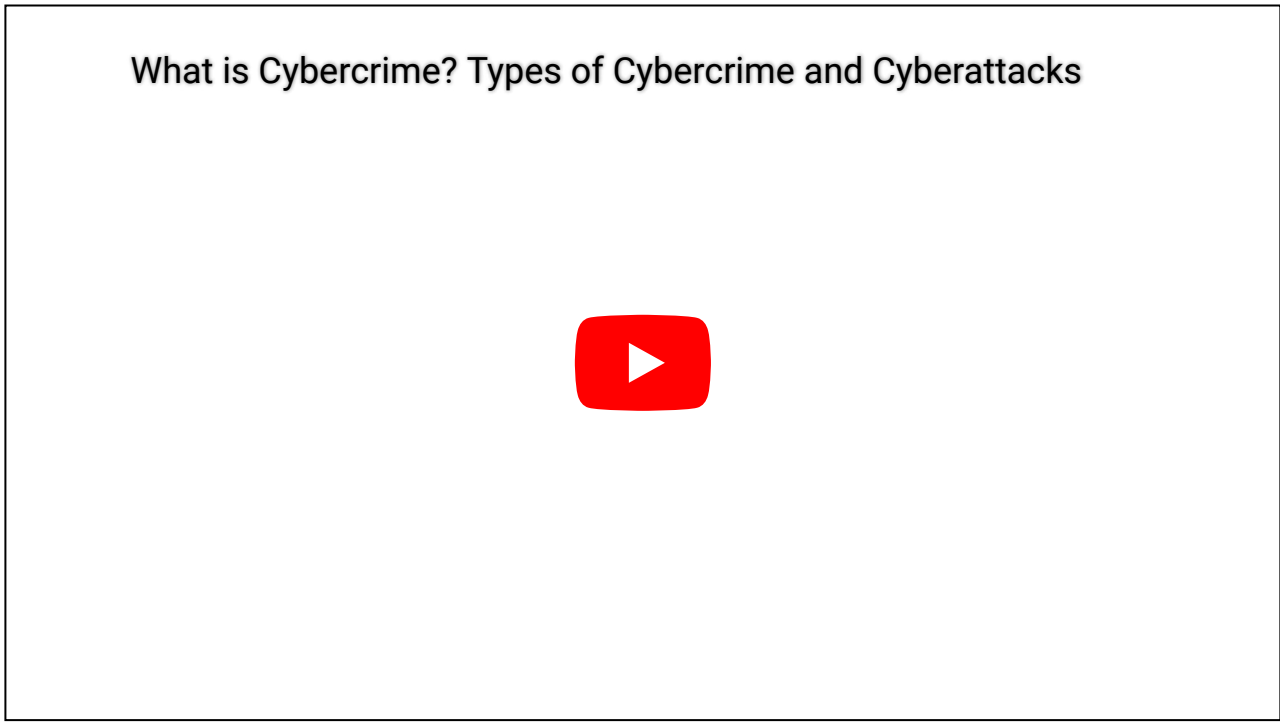
inurl:zoom.us/j and intext:scheduled for

How to prevent Google dork queries

When sensitive information must be protected, it's crucial to prevent dorking. These steps can help:

1. Implement IP-based restrictions and password authentication to protect private areas.
2. Encrypt all sensitive information, like user IDs, passwords, email addresses, phone numbers, etc.
3. Run vulnerability scans to find and disable Google dorks.
4. Run regular dork queries to discover loopholes and sensitive information before attacks occur.

5. Request the removal of sensitive content using Google Search Console.
6. Hide and block sensitive content using the robots.txt file, located in the root-level website directory.



See also: Boolean, search engine results page and organic search results.

This was last updated in September 2022

Continue Reading About Google dork query

- How cyber warfare laws limit risk on a digital battleground
- MVSP: Will Google's security baseline work?
- 13 common types of cyber attacks and how to prevent them
- DOJ report warns of escalating cybercrime, 'blended' threats
- Tackling the post Covid cybercrime pandemic

Related Terms

command-and-control server (C&C server)

A command-and-control server (C&C server) is a computer that issues directives to digital devices that have been infected with ... See complete definition

What is a private cloud?

Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and ... See complete definition

What is the zero-trust security model?

The zero-trust security model is a cybersecurity approach that denies access to an enterprise's digital resources by default and ... See complete definition

SearchNetworking

wireless mesh network (WMN)

A wireless mesh network (WMN) is a mesh network created through the connection of wireless access point (WAP) nodes installed at ...

Wi-Fi 7

Wi-Fi 7 is the pending 802.11be standard under development by IEEE.