

It's time to close the door on open directories

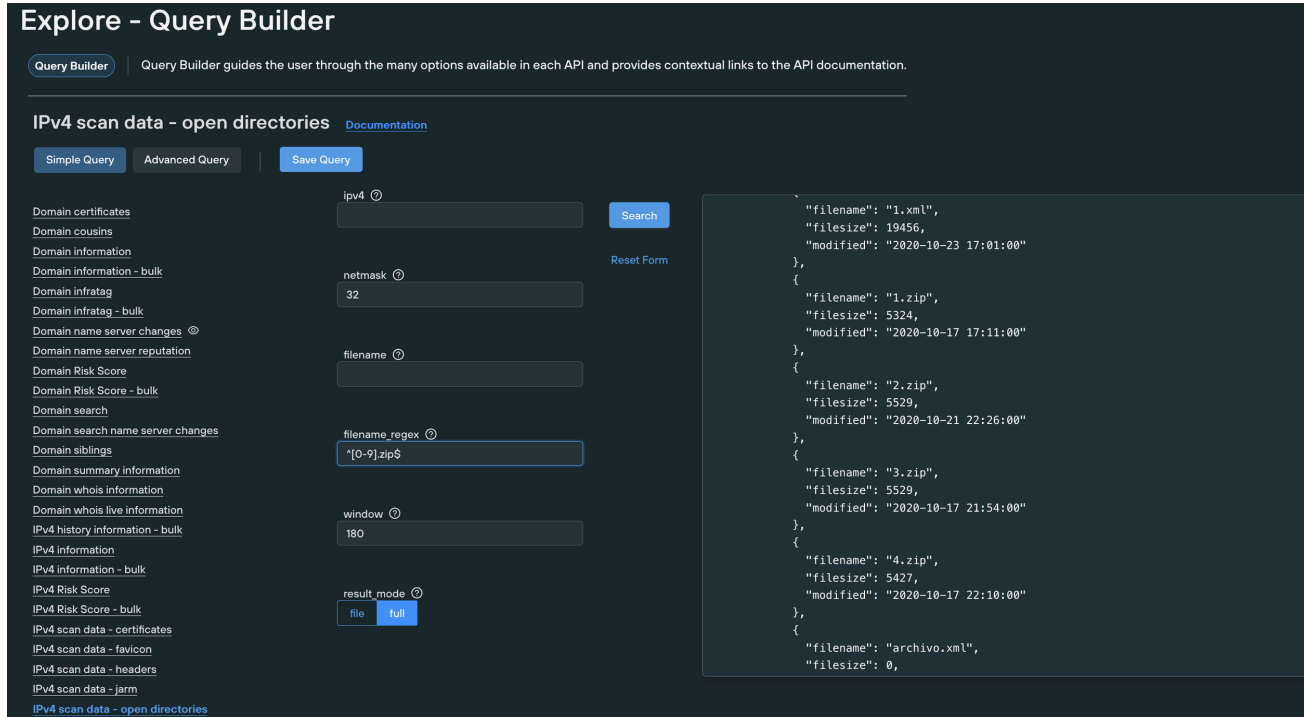
 silentpush.com/blog/its-time-to-close-the-door-on-open-directories

July 21, 2022



Jul 21

Written By [The Team](#)



Explore - Query Builder

Query Builder | Query Builder guides the user through the many options available in each API and provides contextual links to the API documentation.

IPv4 scan data - open directories [Documentation](#)

Simple Query | Advanced Query | Save Query

Search

Reset Form

```
{
  "filename": "1.xml",
  "filesize": 19456,
  "modified": "2020-10-23 17:01:00"
},
{
  "filename": "1.zip",
  "filesize": 5324,
  "modified": "2020-10-17 17:11:00"
},
{
  "filename": "2.zip",
  "filesize": 5529,
  "modified": "2020-10-21 22:26:00"
},
{
  "filename": "3.zip",
  "filesize": 5529,
  "modified": "2020-10-17 21:54:00"
},
{
  "filename": "4.zip",
  "filesize": 5427,
  "modified": "2020-10-17 22:10:00"
},
{
  "filename": "archivo.xml",
  "filesize": 0,

```

Search through indexed directories and files from open directories to help protect your organization.
























Most people have listened to an elderly relative extolling the virtues of the 'good old days', including a semi-smug description of their front door being left open in the summer - usually justified by the fact that they didn't have anything worth stealing.

Open directories are just that - an open door onto your fileserver which, unlike an average 1950s living room, contains information that is extremely valuable, for a variety of reasons.

In the world of global commerce, data is a highly lucrative and sought-after commodity. By using open directories, threat actors are able to seize vast amounts of commercially sensitive information in a matter of seconds, and they're gone before you even know they were there.

Let's take a look at the global problem of open directories, what the consequences are, and how you can find them using the **Silent Push Open Directory Finder**.

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 1.xml	2020-10-23 17:01	19K	
 1.zip	2020-10-17 17:11	5.2K	
 2.zip	2020-10-21 22:26	5.4K	
 3.zip	2020-10-17 21:54	5.4K	
 4.zip	2020-10-17 22:10	5.3K	
 archivo.xml	2020-10-22 00:47	0	
 banco/	2020-12-17 15:26	-	
 beeduk.tar.gz	2020-12-10 13:25	120M	
 certificado.pem	2020-10-21 23:17	4.8K	
 certificado/	2020-10-22 00:28	-	
 copias/	2021-11-05 22:28	-	
 correo/	2021-11-24 23:43	-	
 dian.php	2020-10-22 00:08	9.5K	
 dian/	2021-11-05 22:22	-	
 dian2.php	2021-11-06 19:36	6.5K	
 dian3.php	2021-12-21 19:19	16K	
 imagen.php	2020-10-23 01:23	149	
 kary/	2020-10-14 19:15	-	
 lib.zip	2020-10-22 00:19	148K	
 lib/	2019-06-24 21:06	-	
 mail.private	2021-01-08 04:59	1.6K	
 mail.txt	2021-01-08 04:59	516	
 mailer/	2021-11-16 14:53	-	

An example of an open directory- the full file structure of the server is browsable by anyone on the internet.

What are open directories?

Open directories are freely accessible links to files hosted on a webserver that's connected to the Internet, and not subject to any authentication methods or external access rules.

There's no software-based trickery involved. Open directories can be found using a simple Google search, tailored towards different categories of data. Once a threat actor has identified an open directory, they're free to browse through an organization's file structure without circumnavigating RBAC or permissions-based security measures.

Whilst it is undoubtedly immoral to access and/or download sensitive information that isn't meant for prying eyes, the act of browsing through an open directory is a legal gray area. There's no global consensus on how such scenarios should be legislated against, and sentiments vary from jurisdiction to jurisdiction.

How damaging can they be to your organization?

Very. Extremely. Catastrophically, in fact.

Malicious activity on open directories is nigh on impossible to detect. The first you'll hear of it is either a phone call from a law enforcement/regulatory agency, an email from a hacker demanding money to keep quiet, or a very annoyed customer wondering why their data has been passed around the Internet for the last few years.

Then there's the compliance and liability aspect. Cyber insurance policies don't cover the commercial or operational consequences of an open directory exploit, so unless you have the working capital to deal with the fall-out, it could lead to untold reputational and financial damage and land you in pretty hot regulatory water.

Last, and by no means least, is the data itself. Take a moment to think about the data held on your organization's web servers and file servers, and what would happen if you exposed it to the world through an open directory.

By working with firms to improve their threat resilience, we've seen sensitive data held in open directories that would make a privacy protection lawyer spontaneously combust:

- Full environment files.
- Commercial application configs.
- Cryptowallet logins.
- VPN installers.
- *.xls* and *.docx* files containing PII and GDPR/HIPAA-regulated data.

Once you start investigating open directories on the behalf of large organizations, the horror stories come thick and fast. We recently came across a fairly sizable prison in the USA that left the door open to tens of thousands of electronic prisoner and staff records, including legal information, social security numbers and conviction details.

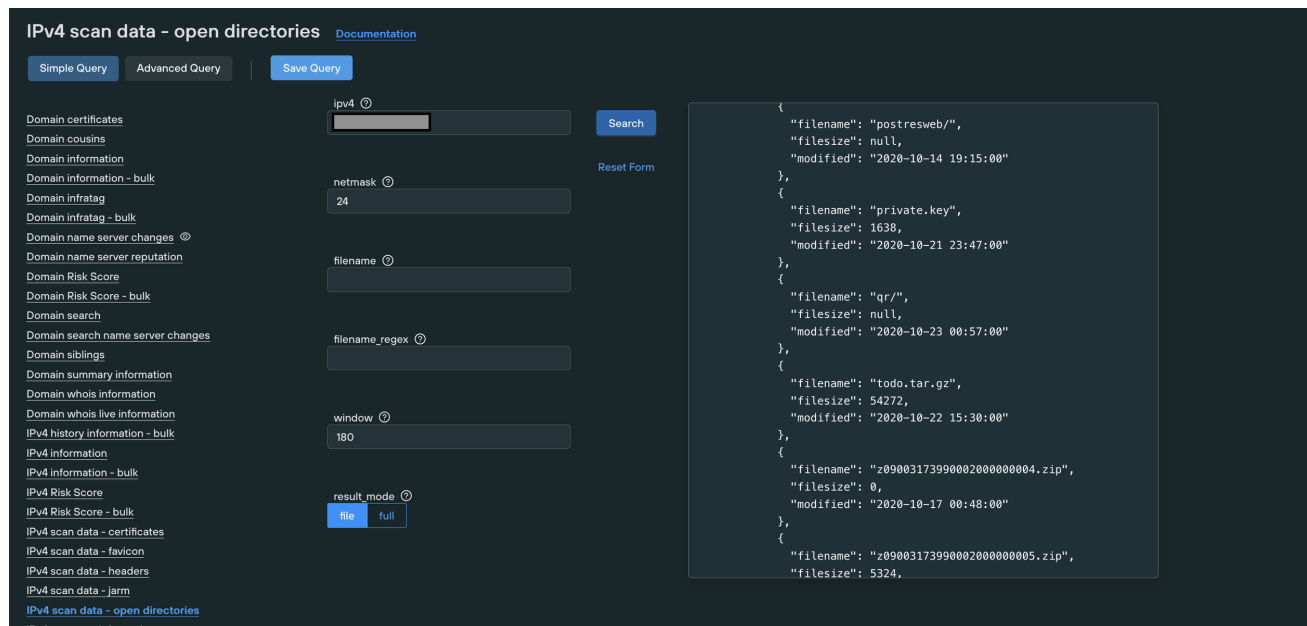
How do you prevent them?

Like other forms of threat protection (such as stopping subdomain takeovers), securing your organization's data by preventing open directories is done through a combination of vigilance and good housekeeping.

Anyone who's ever browsed the Internet has, somewhere along the line, received the dreaded error 403 Forbidden or 404 File Not Found, instead of a web page. As an organization looking to protect its data, these errors are your friends, not your enemies - this is what users are faced with when a server has been configured to block access to directory content.

Methods vary from platform to platform (from simple login controls to modifying your *.htaccess* files and ensuring that IIS is configured correctly), but if you host ANY kind of sensitive data on a webserver, you need to make sure that it's configured so that external and unauthenticated users aren't able to view directory data.

Silent Push Open Directory Finder



Find open directories exposed on your infrastructure or search for your name across all open directories

The **Silent Push Open Directory Finder** searches the global IPv4 range (all 4,294,967,296 addresses) for open directories, to a granular set of parameters that can be configured to your organization's unique requirements.

Our cloud-based platform provides search and filter options (with RE2 regex support) on all known open directories, including variables such as range, partial match and time window. Results can either be outputted in full, or to a file for further interrogation.

If you're a large, multi-site, multi-jurisdictional organization with an extensive online presence, you'll be presented with a realtime list of open directories within the specified range.

Enterprise-level threat monitoring (including open directory detection) doesn't need to be resource hungry. With the right tools, it is quite literally as easy as clicking a few buttons, in order to shore up your commercial data and close the aforementioned door onto your network that leads to something considerably more valuable than your grandmother's collection of faux-porcelain dogs.

The Team