



Bharath

[Follow](#)

Security researcher, Stargazer and a story teller.

Oct 11, 2017 · 8 min read

```
↳$ ldns-walk @ns1.insecuredns.com insecuredns.com
insecuredns.com.      insecuredns.com. A NS SOA TXT RRSIG NSEC DNSKEY
champ.insecuredns.com. A RRSIG NSEC
conference.insecuredns.com. A RRSIG NSEC
damn.insecuredns.com. A RRSIG NSEC
firewall.insecuredns.com. A RRSIG NSEC
mail.insecuredns.com. A RRSIG NSEC
ns1.insecuredns.com. A RRSIG NSEC
ns2.insecuredns.com. A RRSIG NSEC
null.insecuredns.com. A RRSIG NSEC
secrets.insecuredns.com. A RRSIG NSEC
staging.insecuredns.com. A RRSIG NSEC
vpn.insecuredns.com. A RRSIG NSEC
www.insecuredns.com. A RRSIG NSEC
```

## A penetration tester's guide to sub-domain enumeration

As a penetration tester or a bug bounty hunter, most of the times you are given a single domain or a set of domains when you start a security

assessment. You'll have to perform extensive reconnaissance to find interesting assets like servers, web applications, domains that belong to the target organisation so that you can increase your chances of finding vulnerabilities.

*We wrote an extensive [blog post on Open Source Intelligence Gathering techniques](#) that are typically used in the reconnaissance phase.*

Sub-domain enumeration is an essential part of the reconnaissance phase. This blog post covers various sub-domain enumeration techniques in a crisp and concise manner.

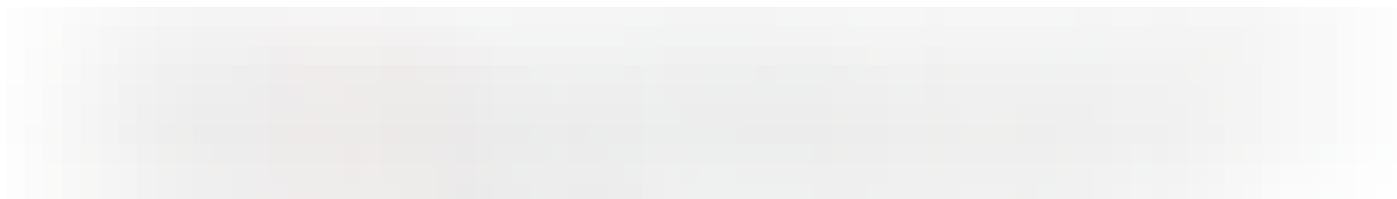
A gitbook will be released as a follow up for this blog post on the same topic where we cover these techniques in-depth. We covered some of these techniques in the “[Esoteric sub-domain enumeration techniques](#)” talk given at Bugcrowd LevelUp conference 2017.

# What is sub-domain enumeration?

Sub-domain enumeration is the process of finding sub-domains for one or more domain(s). It is an essential part of the reconnaissance phase.

## Why sub-domain enumeration?

- Sub-domain enumeration can reveal a lot of domains/sub-domains that are in scope of a security assessment which in turn increases the chances of finding vulnerabilities
- Finding applications running on hidden, forgotten sub-domains may lead to uncovering critical vulnerabilities
- Often times the same vulnerabilities tend to be present across different domains/applications of the same organization

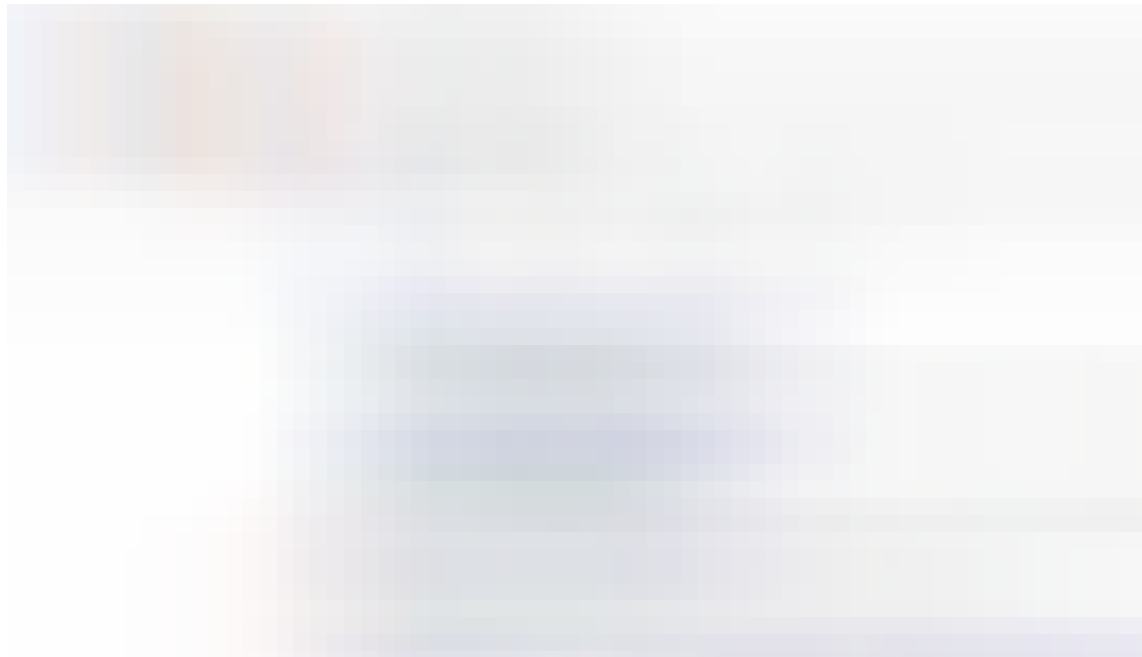


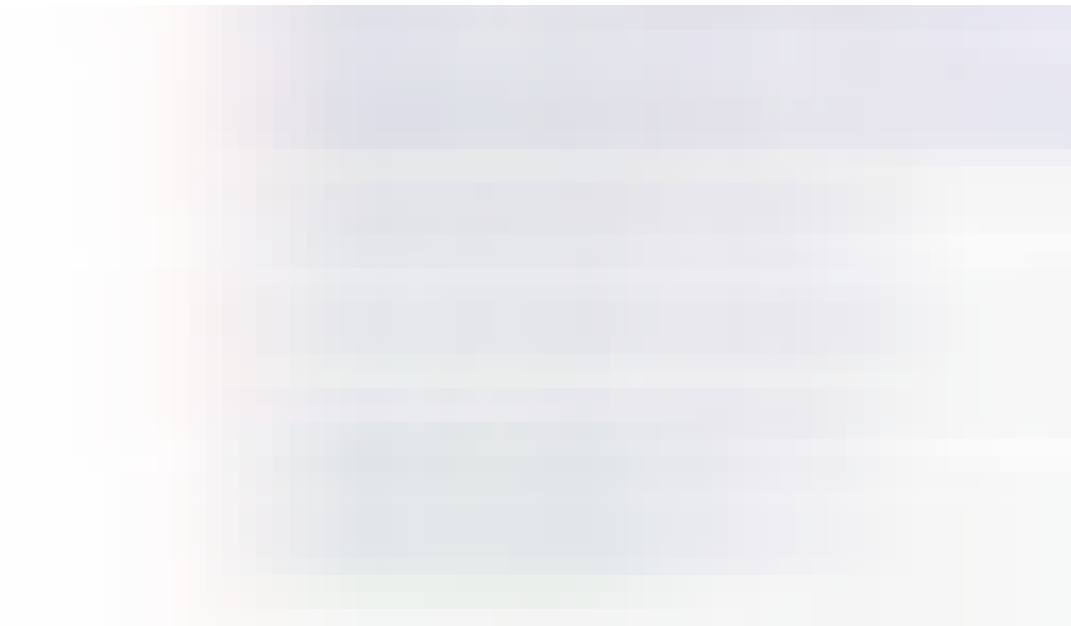
The famous Yahoo! Voices hack happened due to a vulnerable application deployed on a yahoo.com sub-domain

# Sub-domain enumeration techniques

**1.** Search engines like Google and Bing supports various advanced search operators to refine search queries. These operators are often referred to as “Google dorks”.

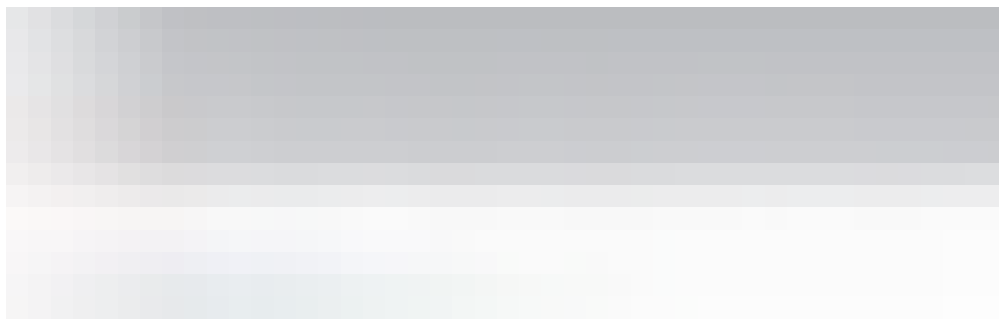
- We can use “**site:**” operator in Google search to find all the sub-domains that Google has found for a domain. Google also supports additional minus operator to exclude sub-domains that we are not interested in “**site:\*.wikimedia.org -www -store -jobs -uk**”

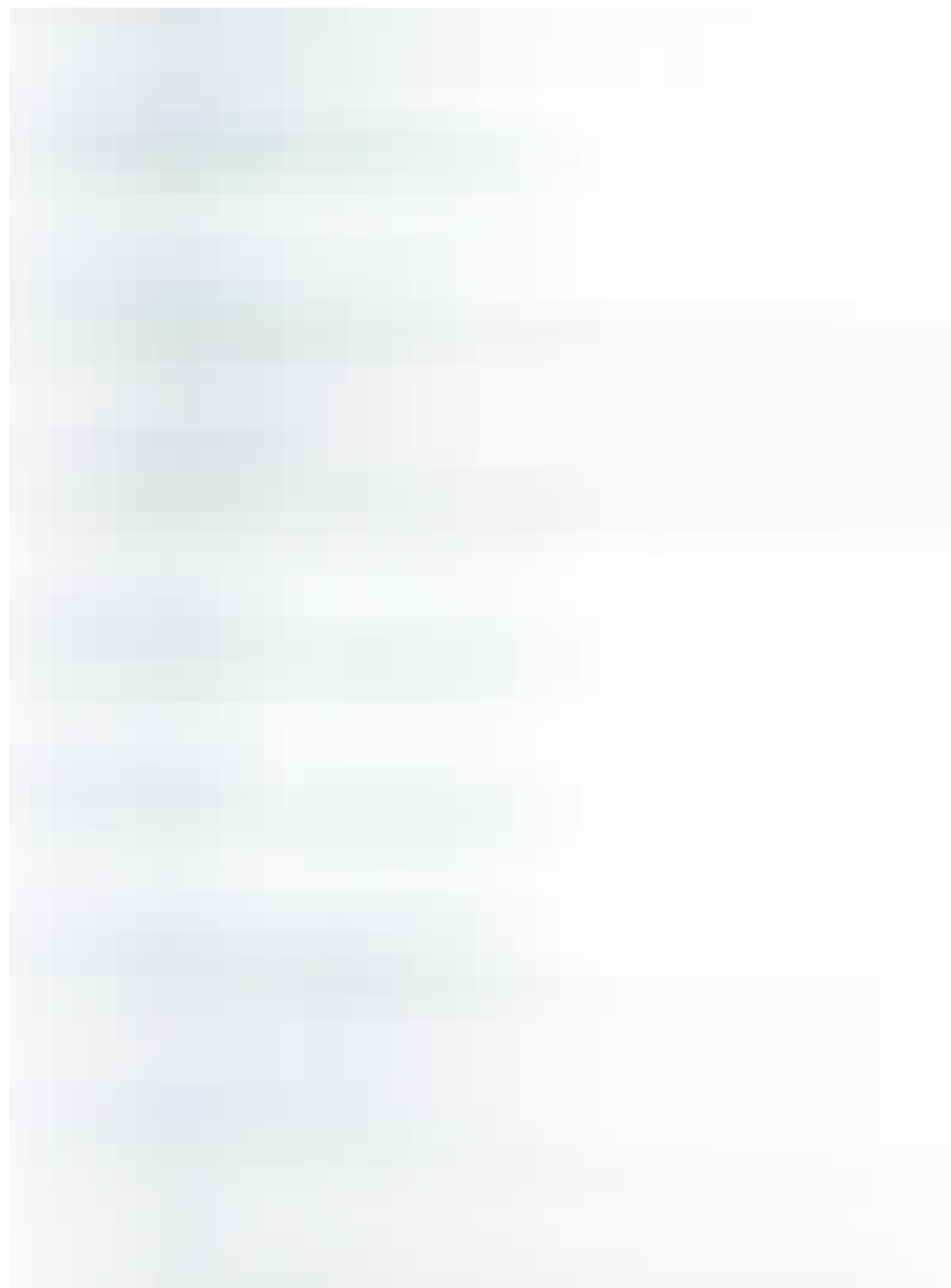




Using **site** operator in Google search to find sub-domains

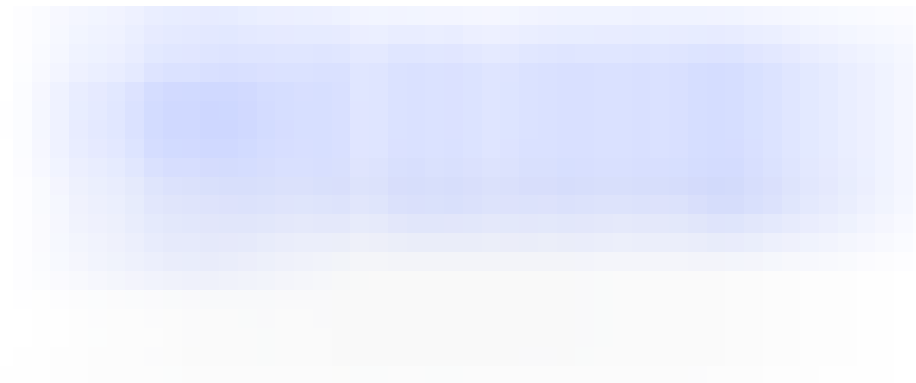
- Bing search engine supports some advanced search operators as well. Like Google, Bing also supports a “**site:**” operator that you might want to check for any additional results apart from the Google search





**2.** There are a lot of the third party services that aggregate massive DNS datasets and look through them to retrieve sub-domains for a given domain.

- VirusTotal runs its own passive DNS replication service, built by storing DNS resolutions performed when visiting URLs submitted by users. In order to retrieve the information of a domain you just have to put domain name in the search bar





Searching for sub-domains using virustotal

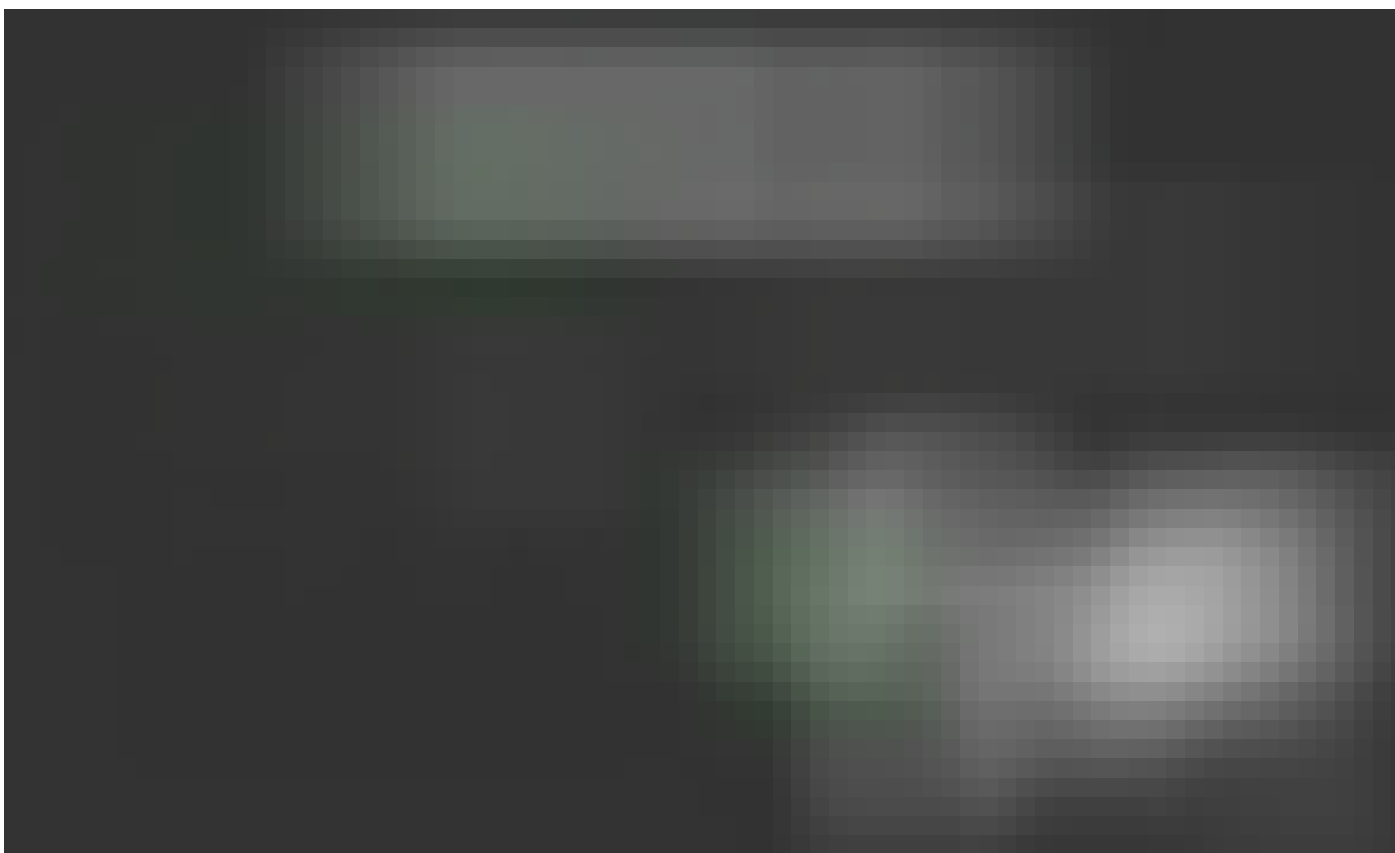




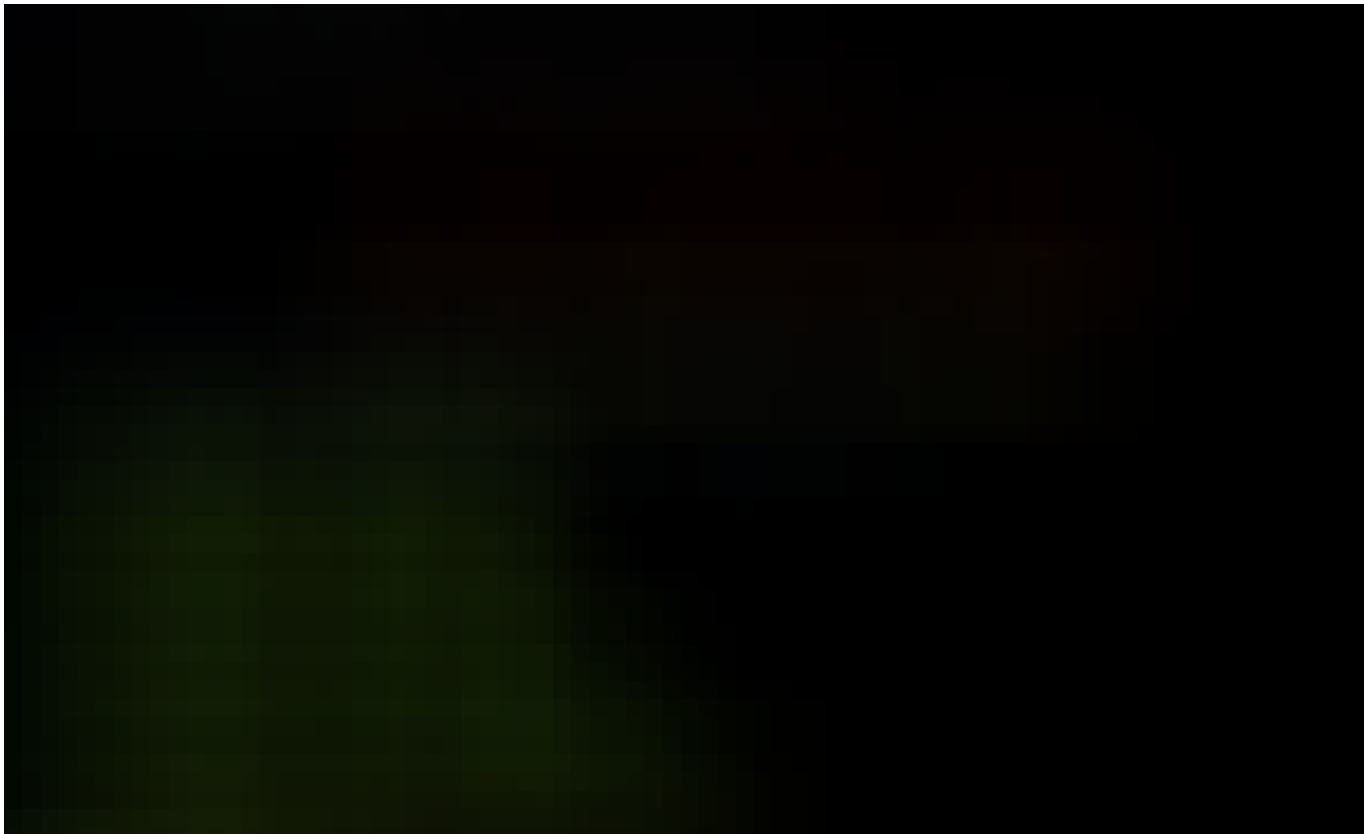


sub-domains found using VirusTotal

- DNSdumpster is another interesting tool that can find potentially large number of sub-domains for a given domain



*Sublist3r is a popular tool that'll enumerate sub-domains using various sources. Sublist3r enumerates sub-domains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates sub-domains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS.*





sub-domain enumeration using **Sublist3r**

**3.** Certificate Transparency(CT) is a project under which a Certificate Authority(CA) has to publish every SSL/TLS certificate they issue to a public log. An SSL/TLS certificate usually contains domain names, sub-domain names and email addresses. This makes them a treasure trove of information for attackers. I wrote a series of technical blog posts on Certificate Transparency where I covered this technique in-depth, you can read the series [here](#).

The easiest way to lookup certificates issued for a domain is to use search engines that collect the CT logs and let's anyone search through them. Few of the popular ones are listed below -

1. <https://crt.sh/>
2. <https://censys.io/>
3. <https://developers.facebook.com/tools/ct/>

4. <https://google.com/transparencyreport/https/ct/>



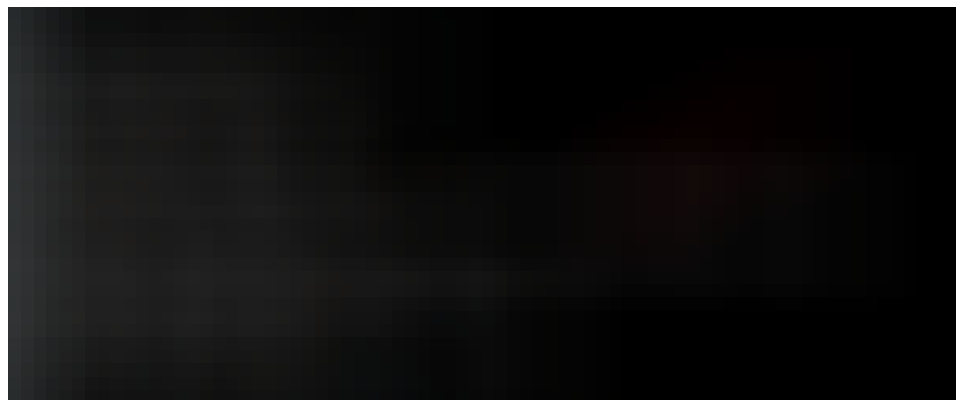
Finding sub-domains of an organisation's primary domain using [crt.sh](https://crt.sh)

Additional to the web interface, crt.sh also provides access to their CT logs data using postgres interface. This makes it easy and flexible to run some advanced queries. If you have the PostgreSQL client software installed, you can login as follows:

```
$ psql -h crt.sh -p 5432 -U guest certwatch
```

We wrote few scripts to simplify the process of finding sub-domains using CT log search engines. The scripts are available in our github repo—

<https://github.com/appsecco/the-art-of-subdomain-enumeration>

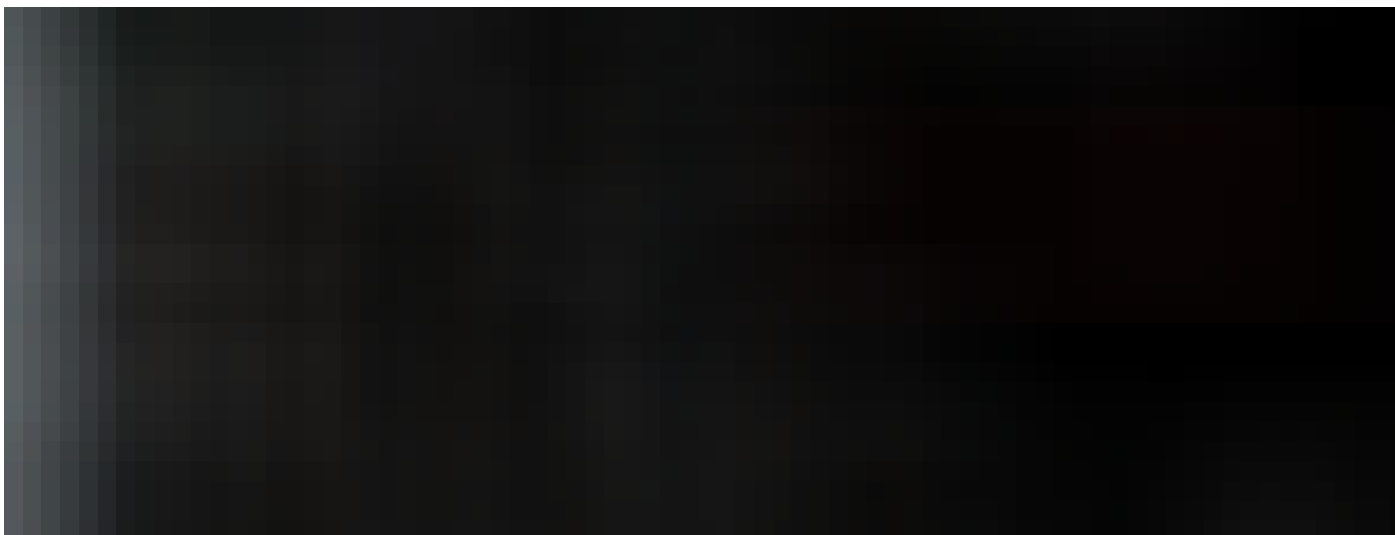


Interesting sub-domain entry from CT logs for uber.com

*The downside of using CT for sub-domain enumeration is that the domain names found in the CT logs may not exist anymore and thus they can't be resolved to an IP address. You can use tools like massdns in conjunction with CT logs to quickly identify resolvable domain names.*

```
# ct.py - extracts domain names from CT Logs (shipped with massdns)
# massdns - will find resolvable domains & adds them to a file

./ct.py icann.org | ./bin/massdns -r resolvers.txt -t A -q -a -o -w
icann_resolvable_domains.txt -
```



Using massdns to find resolvable domain names

**4.** Dictionary based enumeration is another technique to find sub-domains with generic names. DNSRecon is a powerful DNS enumeration tool, one of its features is to conduct dictionary based sub-domain enumeration using a pre-defined wordlist.

```
$ python dnsrecon.py -n ns1.insecuredns.com -d insecuredns.com -D  
subdomains-top1mil-5000.txt -t brt
```



Dictionary based enumeration using DNSRecon

**5.** Permutation scanning is another interesting technique to identify sub-domains. In this technique, we identify new sub-domains using permutations, alterations and mutations of already known domains/sub-domains.

- Altdns is a tool that allows for the discovery of sub-domains that conform to patterns

```
$ python altdns.py -i icann.domains -o data_output -w icann.words -r  
-s results_output.txt
```



Finding sub-domains that match certain permutations/alterations using AltDNS

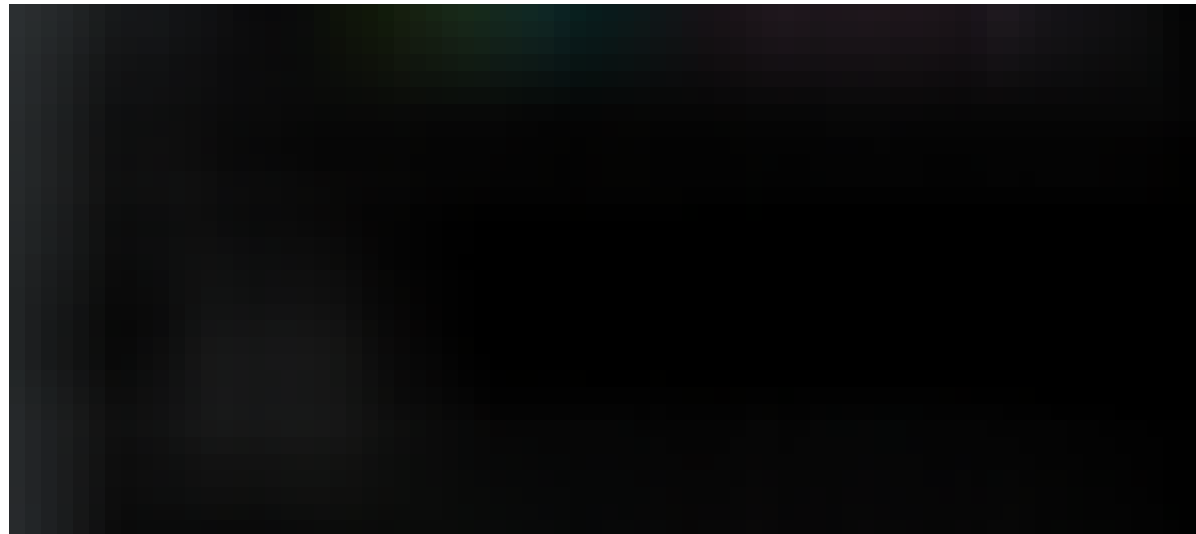
**6.** Finding Autonomous System (AS) Numbers will help us identify netblocks belonging to an organization which in-turn may have valid domains.

- Resolve the IP address of a given domain using `dig` or `host`
- There are tools to find ASN given an IP address—  
<https://asn.cymru.com/cgi-bin/whois.cgi>
- There are tools to find ASN given a domain name—<http://bgp.he.net/>



- The ASN numbers found can be used to find netblocks of the domain.  
There are Nmap scripts to achieve that—  
<https://nmap.org/nsedoc/scripts/targets-asn.html>

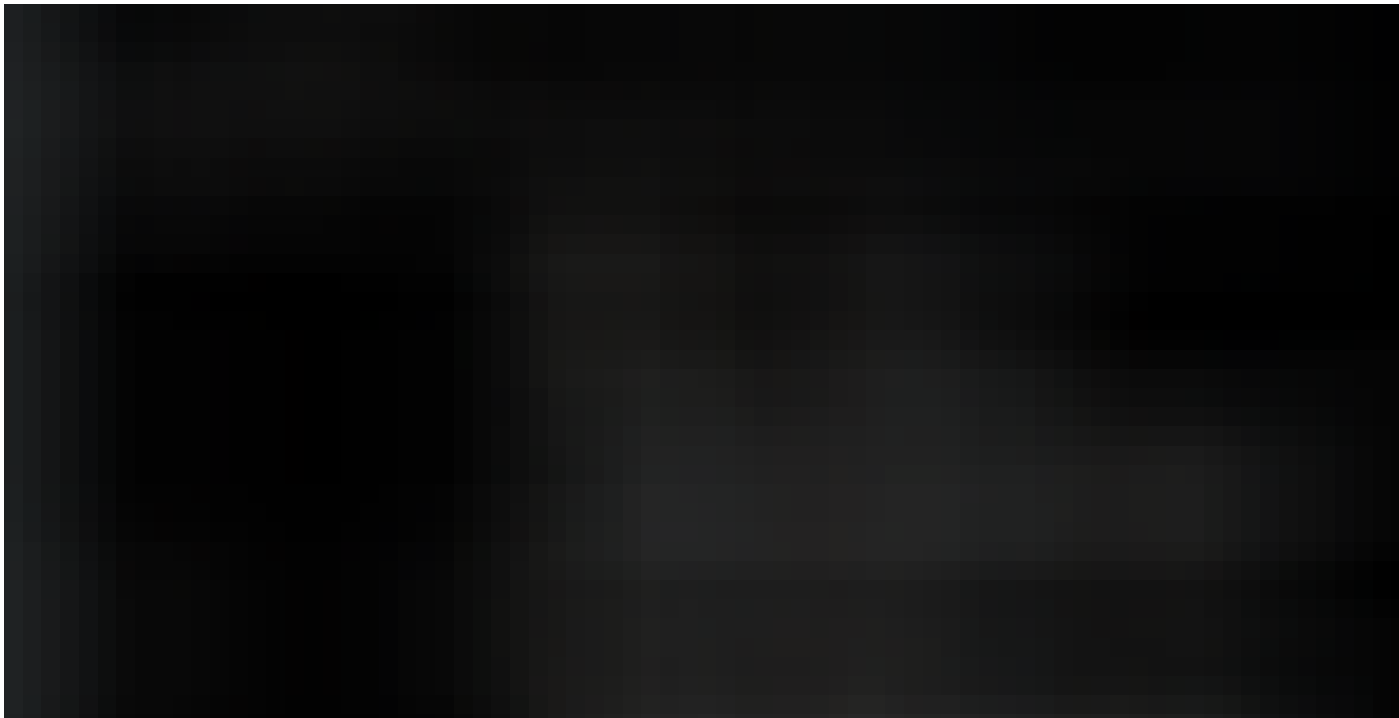
```
$ nmap --script targets-asn --script-args targets-asn.asn=17012 >  
netblocks.txt
```



Finding netblocks using AS numbers—NSE script

**7.** Zone transfer is a type of DNS transaction where a DNS server passes a copy of full or part of its zone file to another DNS server. If zone transfers are not securely configured, anyone can initiate a zone transfer against a nameserver and get a copy of the zone file. By design, zone file contains a lot of information about the zone and the hosts that reside in the zone.

```
$ dig +multi AXFR @ns1.insecuredns.com insecuredns.com
```



Successful zone transfer using DIG tool against a nameserver for a domain

**8.** Due to the way non-existent domains are handled in DNSSEC, it is possible to “walk” the DNSSEC zones and enumerate all the domains in that zone. You can learn more about this technique from [here](#).

- For DNSSEC zones that use NSEC records, zone walking can be performed using tools like *ldns-walk*

```
$ ldns-walk @ns1.insecuredns.com insecuredns.com
```

## Zone walking DNSSEC zone with NSEC records

- Some DNSSEC zones use NSEC3 records which uses hashed domain names to prevent attackers from gathering the plain text domain names. An attacker can collect all the sub-domain hashes and crack the hashes offline
- Tools like *nsec3walker*, *nsec3map* help us automate the collecting NSEC3 hashes and cracking the hashes. Once you install *nsec3walker*, you can use the following commands to enumerate sub-domains of NSEC3 protected zone

```
# Collect NSEC3 hashes of a domain
$ ./collect icann.org > icann.org.collect

# Undo the hashing, expose the sub-domain information.
$ ./unhash < icann.org.collect > icann.org.unhash

# Listing only the sub-domain part from the unhashed data
$ cat icann.org.unhash | grep "icann" | awk '{print $2;}'
del.icann.org.
```

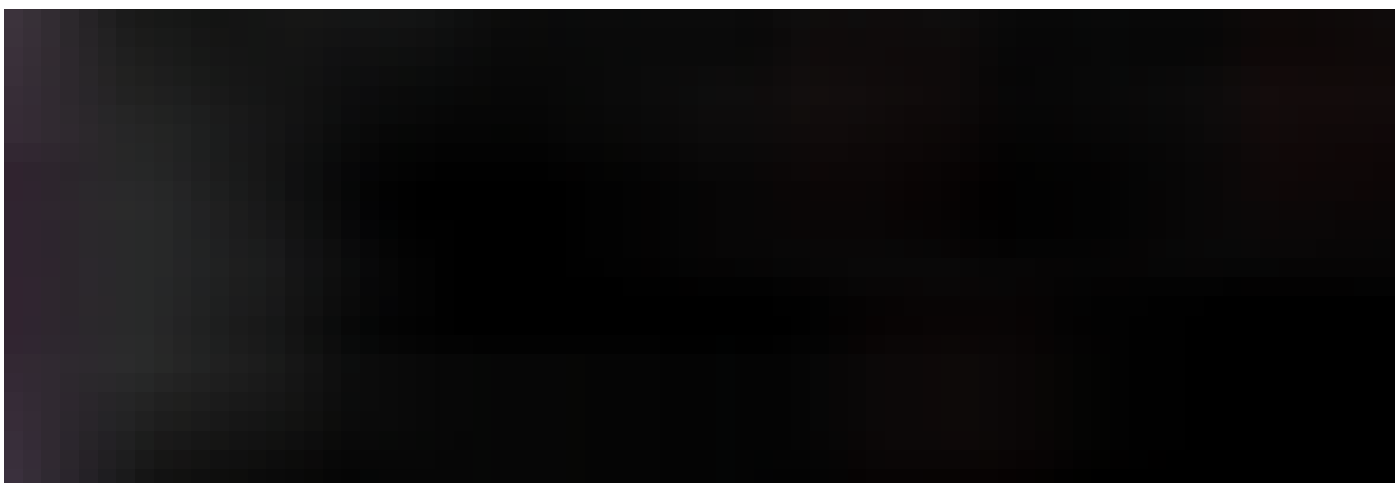
```
access.icann.org.  
charts.icann.org.  
communications.icann.org.  
fellowship.icann.org.  
files.icann.org.  
forms.icann.org.  
mail.icann.org.  
maintenance.icann.org.  
new.icann.org.  
public.icann.org.  
research.icann.org.
```

**9.** There are projects that gather Internet wide scan data and make it available to researchers and the security community. The datasets published by this projects are a treasure trove of sub-domain information. Although finding sub-domains in this massive datasets is like finding a needle in the haystack, it is worth the effort.

- *Forward DNS* dataset is published as part of Project Sonar. This data is created by extracting domain names from a number of sources and then sending an `ANY` query for each domain. The data format is a gzip-compressed JSON file. We can parse the dataset to find sub-domains for a

given domain. The dataset is massive though(20+ GB compressed, 300+ GB uncompressed)

```
# Command to parse & extract sub-domains for a given domain  
  
$ curl -silent https://scans.io/data/rapid7/sonar.fdns\_v2/20170417-fdns.json.gz | pigz -dc | grep ".icann.org" | jq
```



Enumerating sub-domains using FDNS dataset

## Sub-domain enumeration techniques—A comparison

We ran few of the discussed techniques against *icann.org* and compared the results. The bar chart below shows the number of *unique, resolvable sub-domains* each technique found for *icann.org*. Feel free to get in touch with us to know the methods we used to gather this information.



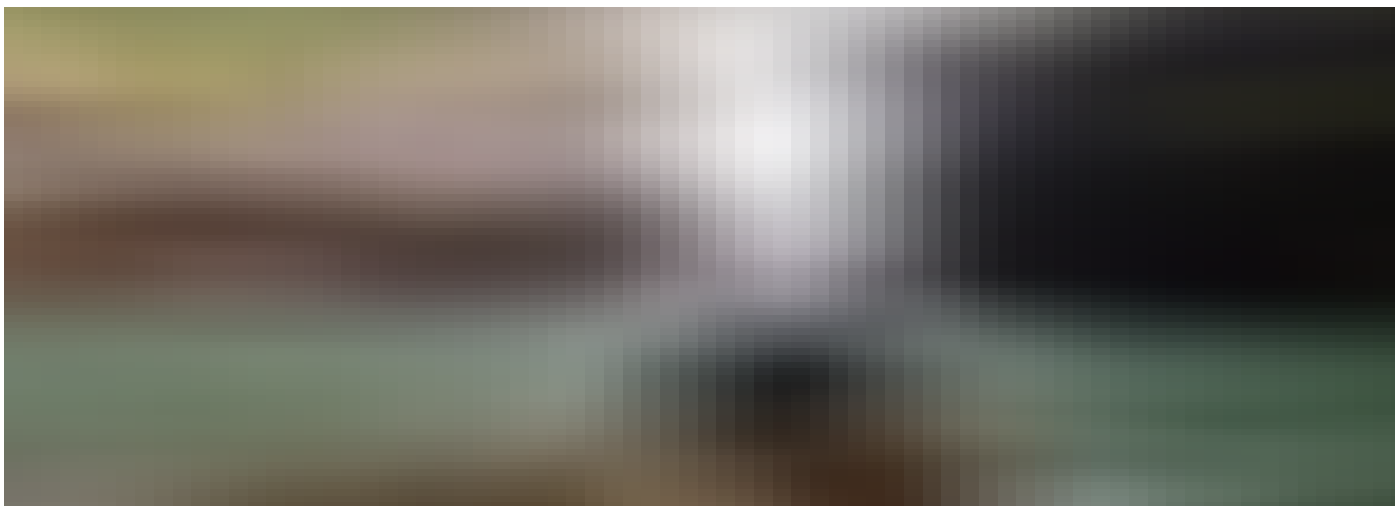


Number of unique, resolvable sub-domains each technique found for icann.org

## Sub-domain enumeration—Reference

We created a simple reference for sub-domain enumeration techniques, tools and sources. This reference is created using a Github gist, feel free to fork, customise it—

<https://gist.github.com/yamakira/2a36d3ae077558ac446e4a89143c69ab>



Quick reference for sub-domain enumeration



## References

- <https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration>
- <https://blog.appsecco.com/open-source-intelligence-gathering-101-d2861d4429e3>
- <https://www.databreaches.net/hackers-post-450k-credentials-apparently-pilfered-from-yahoo/>
- <http://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt>
- <https://www.peerlyst.com/posts/bsideslv-2017-breaking-ground-with-underflow-bsides-las-vegas>

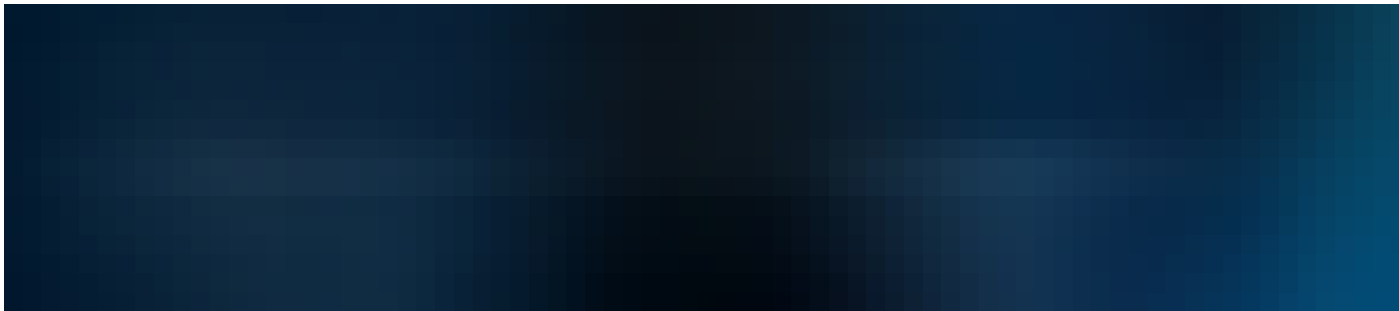
. . .

**Thank you for reading this article. If you enjoyed it please let us know by clicking that little clap icon below.**

. . .

*At Appsecco we provide advice, testing, training and insight around software and website security, especially anything that's online, and its associated hosting infrastructure—Websites, e-commerce sites, online platforms, mobile technology, web-based services etc.*

*If something is accessible from the internet or a person's computer we can help make sure it is safe and secure.*



DNS

Osint

Application Security

Domain Hacking

Penetration Testing

**Like what you read? Give Bharath a round of applause.**

From a quick cheer to a standing ovation, clap to show how much you enjoyed this story.

1.1K





**Bharath**

Security researcher, Stargazer and a story teller.

Follow




**Appsecco**

Follow

Making sense of application security for everyone. Follow us to get a pragmatic view of the landscape including hacks, attacks, modern defence techniques. We cover ideas on securing applications, training the modern workforce in secure development and testing.

### Responses

 Write a response...

Conversation with [Bharath](#).



**Nabeel Yoosuf**

Nov 13, 2017

A very informative article. Thank you. Did you try Farsight's passive DNS feed (formerly DNSDB)? I am curious to see how it compares to Forward DNS data source from Project Sonar.

1 response 



Bharath

Nov 14, 2017

I did not try Farsight's passive DNS feed. As far as I know, it is a paid service. It'd like to look at a comparison between these datasets. Let me know if you figure it out.



Show all responses