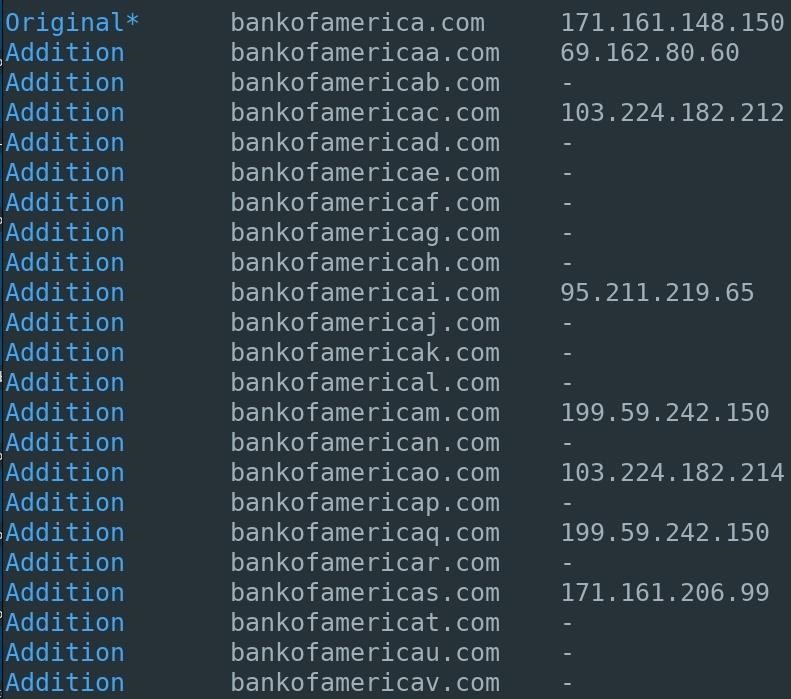
Supported Naming Schemes

Dsntwist supports a variety of phishing domain schemes and types which are used to generate a vast selection of potential phishing domains. I'll cover each below before jumping right into the how-to.

1Addition

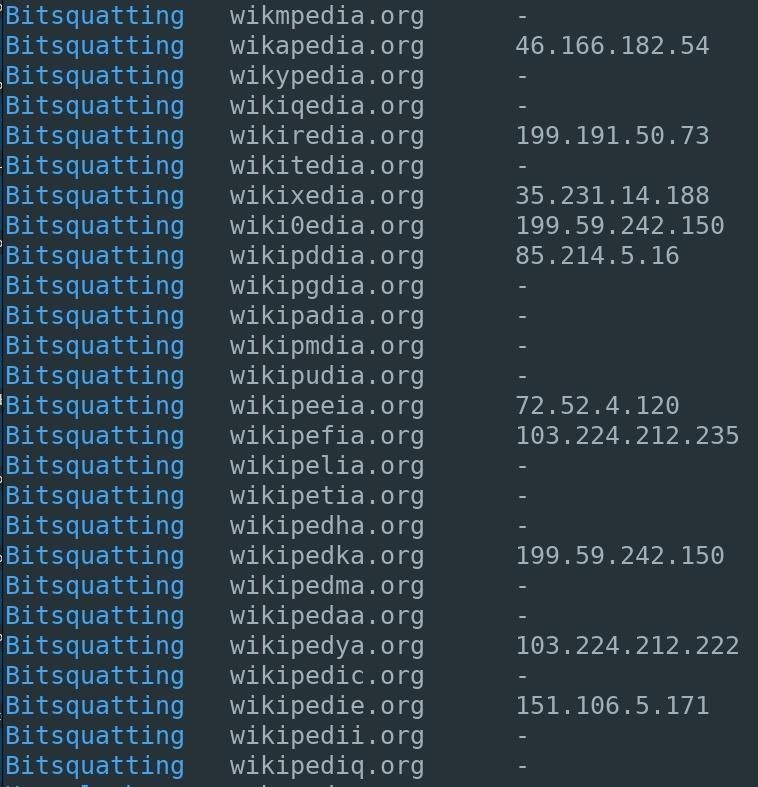
Letters are appended to the end of the given domain name. Below is an example of Bank of America, one of the largest banks in the United States. Unlike some of the other options below, a simple addition is easy enough to spot by an end user if he or she just glances at the URL.

[](https://img.wonderhowto.com/img/original/44/89/63659590049548/0/636595900495484489.jpg)

2Bitsquatting

Bitsquatting refers to the registration of a domain names 1-bit different from a legitimate domain. Below is an example for Wikipedia, the largest and most popular general reference website on the internet. This is a little trickier on the eyes than the "additions" above since a lot of people [read words based on the first and last letter](https://www.mrc-cbu.cam.ac.uk/people/matt.davis/cmabridge/)and don't look at every letter individually.

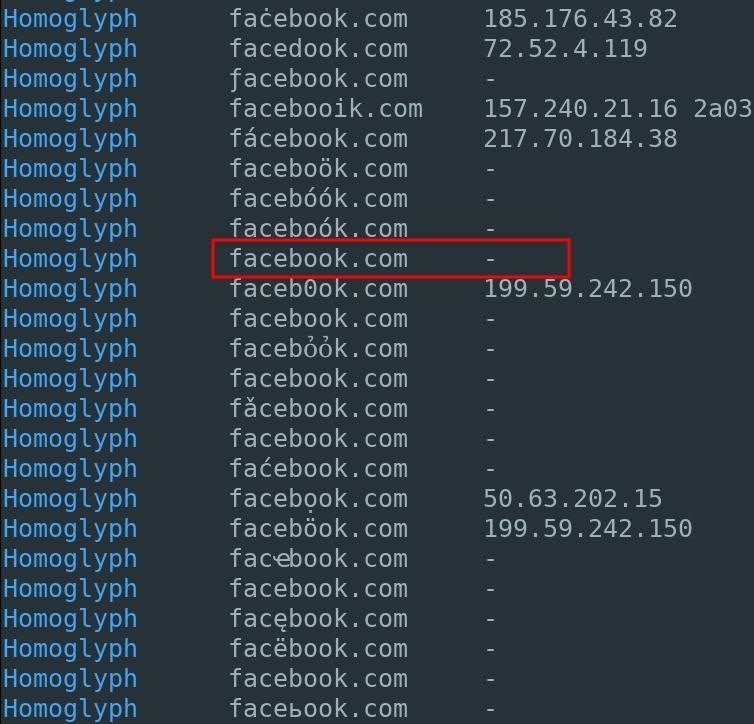
Don't Miss: [Use Leaked Password Databases to Create Brute-Force Wordlists](https://null-byte.wonderhowto.com/how-to/use-leaked-password-databases-create-brute-force-wordlists-0184006/)

[](https://img.wonderhowto.com/img/original/73/13/63659590069704/0/636595900697047313.jpg)

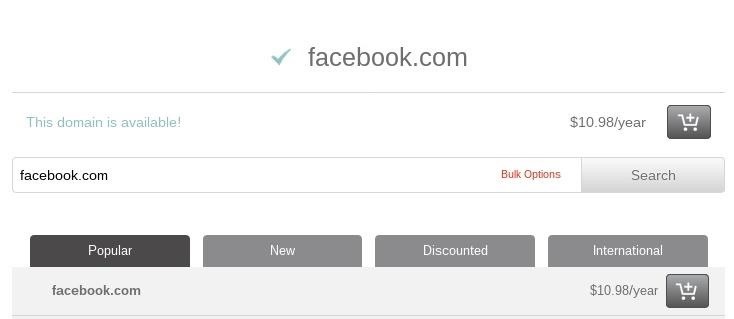
3Homoglyph

Phishing campaigns using homoglyphs are referred to as [homograph attacks](https://null-byte.wonderhowto.com/news/impossible-identify-website-phishing-attack-leaves-chrome-firefox-users-vulnerable-but-you-can-prevent-it-0177172/), even though the alternative characters are referred to as homoglyphs and not homographs. These type of attacks still affect Firefox and most Android devices, and were recently made famous by [Xudong Zheng](https://www.xudongz.com/blog/2017/idn-phishing/" \t "_blank), who created [the first homoglyph phishing address](https://null-byte.wonderhowto.com/news/impossible-identify-website-phishing-attack-leaves-chrome-firefox-users-vulnerable-but-you-can-prevent-it-0177172/) for [apple.com](https://www.apple.com/). Using Facebook as an example, I found there were many homoglyph phishing domains still available for as little as $11.

Don't Miss: [Ways to Crack a Facebook Password & How to Protect Yourself from Them](https://null-byte.wonderhowto.com/how-to/4-ways-crack-facebook-password-protect-yourself-from-them-0139532/)

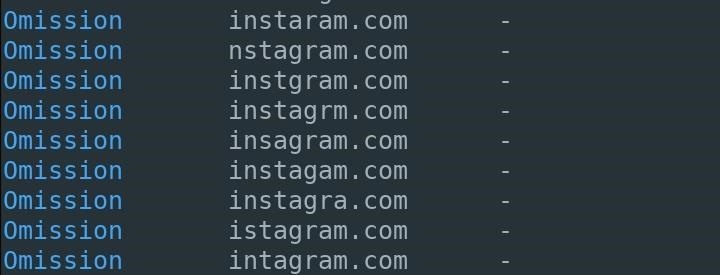
[](https://img.wonderhowto.com/img/original/19/90/63659590087142/0/636595900871421990.jpg)

To check the discovered domain name against a domain registrar, copy and paste the domain from the Dnstwist terminal into the registrar's search bar.

[](https://img.wonderhowto.com/img/original/42/31/63659590105048/0/636595901050484231.jpg)

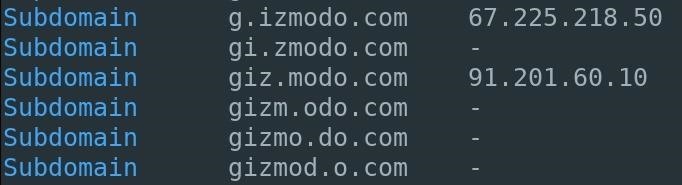
4Omission

Letters are simply removed from the domain name. To my surprise, all of the Instagram domain names were listed as available. While someone will probably notice if the first or last letter in the domain name is missing, they might not notice one in the middle gone.

[](https://img.wonderhowto.com/img/original/97/16/63659590123985/0/636595901239859716.jpg)

5Subdomain

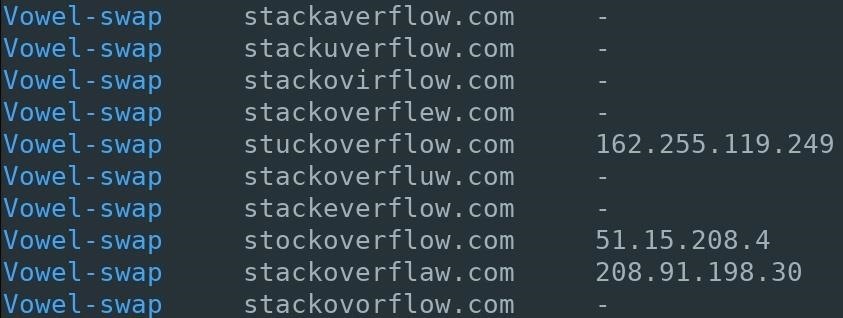
A period inserted at varying positions in the given domain name. Using Gizmodo as an example, we can see the domains "odo.com" and "zmodo.com" are available. It's just a matter of creating convincing subdomains to make an effective phishing domain. Like "additions," this might be more obvious than the other tricks here.

[](https://img.wonderhowto.com/img/original/69/00/63659590141829/0/636595901418296900.jpg)

6Vowel-Swap

Vowels found in the given domain are swapped for different vowels. At a glance, many of these domains will likely fool most victims into clicking on fraudulent links. Again, this works since most people scan words using the first and last letter, not necessarily every letter in the middle. If a replaced vowel is the first or last letter, it probably won't work as well.

Don't Miss: [Find Anyone's Private Phone Number Using Facebook](https://null-byte.wonderhowto.com/how-to/find-anyones-private-phone-number-using-facebook-0181071/)

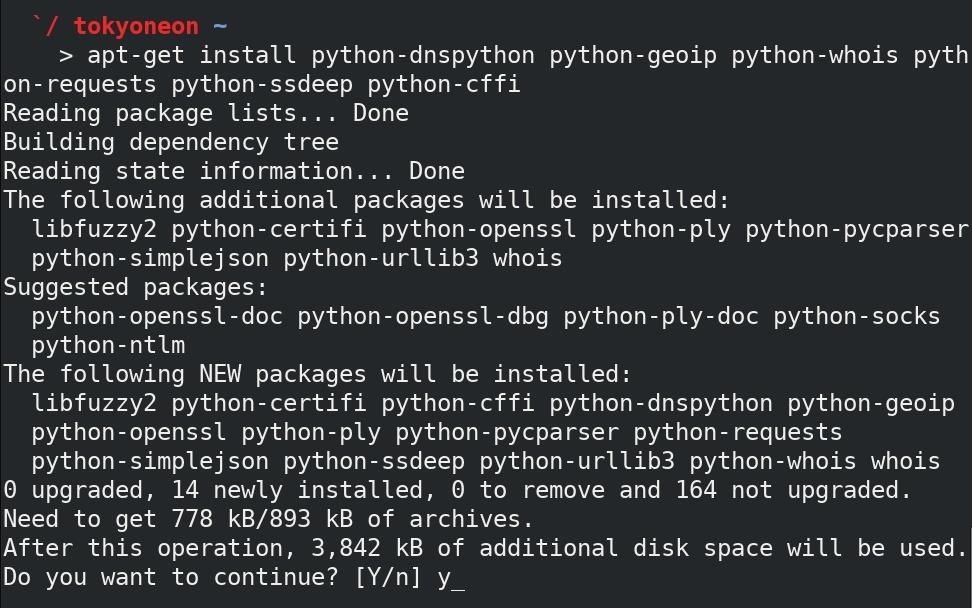
[](https://img.wonderhowto.com/img/original/17/72/63659590159142/0/636595901591421772.jpg)

Now that you know all of the tricks Dnstwist can use to find used and available phishing domains, let's see how to actually use the tool.

Step 1Set Up Dnstwist

Dnstwist relies on several Python dependencies which can be installed in [Kali Linux](https://tag.wonderhowto.com/how-to-do-kali/)by typing the below command into a terminal.

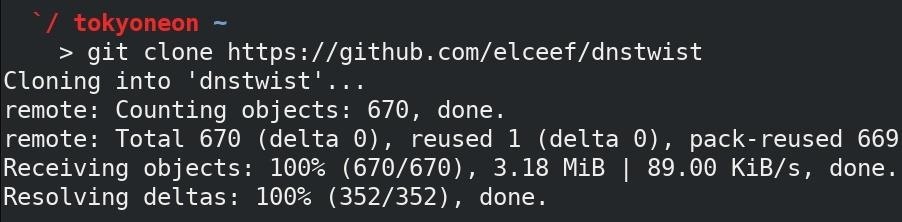
[apt-get](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-5-installing-new-software-0147591/) install python-dnspython python-geoip python-whois python-requests python-ssdeep python-cffi

[](https://img.wonderhowto.com/img/original/71/39/63659590177079/0/636595901770797139.jpg)

Next, clone the [Dnstwist GitHub repository](https://github.com/elceef/dnstwist" \t "_blank).

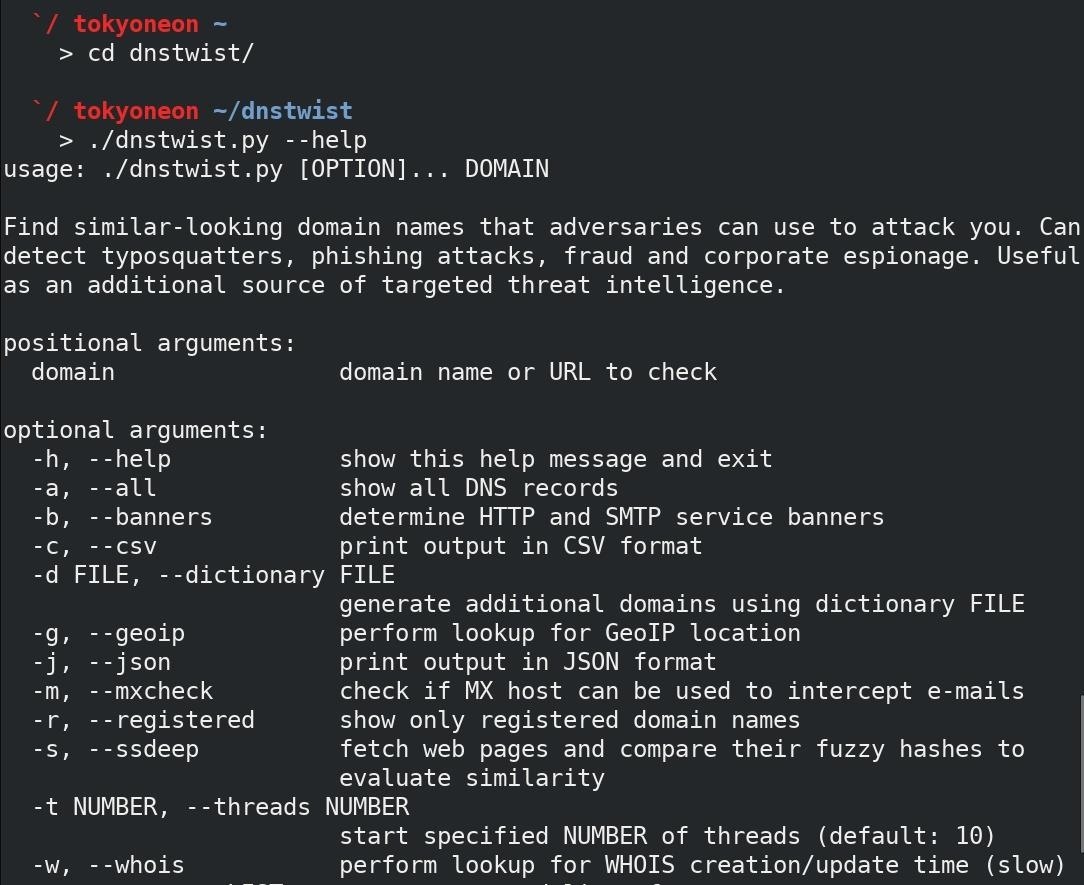
git clone https://github.com/elceef/dnstwist

Don't Miss: [How to Use Git to Clone, Compile & Refine Open-Source Hacking Tools](https://null-byte.wonderhowto.com/how-to/mac-for-hackers-use-git-clone-compile-refine-open-source-hacking-tools-0174254/)

[](https://img.wonderhowto.com/img/original/86/89/63659590194454/0/636595901944548689.jpg)

Finally, use the [**cd**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-2-creating-directories-files-0147234/) command to change into the newly create "dnstwist" directory and use the command underneath it to view the available options.

cd dnstwist/  
./dnstwist.py --help

[](https://img.wonderhowto.com/img/original/68/62/63659590220454/0/636595902204546862.jpg)

Step 2Generate Phishing Domains with Dnstwist

To start generating phishing domains with Dnstwist, use the below command. There are several arguments being utilized in my example command, so jump down under the screenshot to see a quick breakdown.

./dnstwist.py --ssdeep --json --threads 40 website.com > website.com.json

[](https://img.wonderhowto.com/img/original/72/21/63659590240829/0/636595902408297221.jpg)

Don't Miss: [Easily Detect CVEs with Nmap Scripts](https://null-byte.wonderhowto.com/how-to/easily-detect-cves-with-nmap-scripts-0181925/)

* The **--ssdeep** argument instructs Dnstwist to analyze the HTML found on each domain and compare it to the HTML of the given (real) website. The level of similarity will be expressed as a percentage. However, each website should be inspected manually regardless of the percentage level issued by Dnstwist. These percentages are merely there to aid security professionals in identifying which domains are most likely to be phishing domains.
* Dnstwist supports two output formats which can be used with other applications. The **--json** output format was used in my above example but there's also support for CSV outputs which can be enabled using the **--cvs**argument instead of the JSON format. To save either format to a file, the **> filename** redirect can be used to write the data to a given filename.
* By default, Dnstwist will make only 10 requests at a time when enumerating available phishing domains. This number can be increased or decreased using the **--threads** argument and specifying a value.

A progress bar will print at the bottom of the Dnstwist terminal. Depending on network speed and number of threads, this can take several minutes to complete.