m57 / **dnsteal**

Watch 52 Star 643 Fork 91

DNS Exfiltration tool for stealthily sending files over DNS requests.

21 commits **1** branch **0** releases **2** contributors

Branch: **master** New pull request New file Find file HTTPS https://github.com/m57/dr Download ZIP

m57 test_commit Latest commit 634fee8 Jan 12, 2016

LICENSE	Initial commit	Aug 11, 2015
README.md	Stupid readme fix	Oct 22, 2015
dnsteal.py	test_commit	Jan 12, 2016

README.md

dnsteal v 2.0

This is a fake DNS server that allows you to stealthily extract files from a victim machine through DNS requests.

Below are a couple of different images showing examples of multiple file transfer and single verbose file transfer:

- Support for multiple files
- Gzip compression supported
- Now supports the customisation of subdomains and bytes per subdomain and the length of filename

See help below:

If you do not understand the help, then just use the program with default options!

```
python dnsteal.py 127.0.0.1 -z -v
```

This one would send 45 bytes per subdomain, of which there are 4 in the query. 15 bytes reserved for filename at the end.

```
python dnsteal.py 127.0.0.1 -z -v -b 45 -s 4 -f 15
```

This one would leave no space for filename.

```
python dnsteal.py 127.0.0.1 -z -v -b 63 -s 4 -f 0
```

~x90