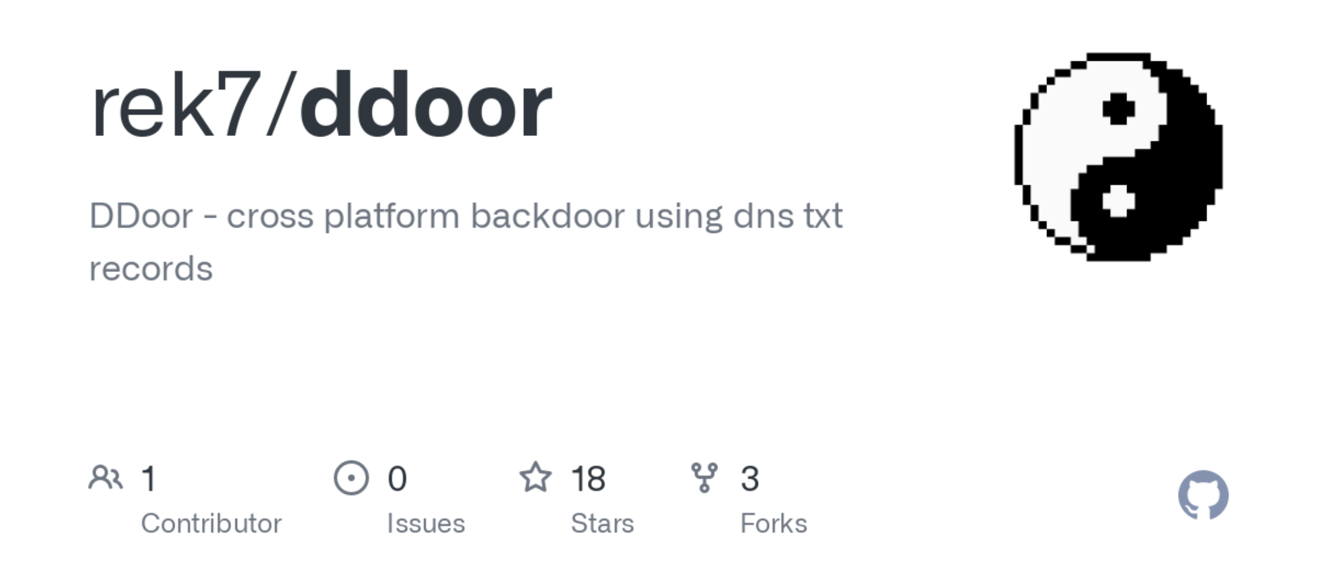
ddoor

github.com/rek7/ddoor

rek7



rek7/ddoor

DDoor - cross platform backdoor using dns txt records

cross platform backdoor using dns txt records

What is ddor?

ddor is a cross platform light weight backdoor that uses txt records to execute commands on infected machines.

Features

- Allows a single txt record to have seperate commands for both linux and windows machines
- List of around 10 public DNS servers that it randomly chooses from
- Unpredictable call back times
- Encrypts txt record using xor with custom password
- Supports DNS over HTTPS (Shoutout to Keith @keharv for adding this!)

Linux Features:

- Anti-Debugging, if ptrace is detected as being attached to the process it will exit.
- Process Name/Thread names are cloaked, a fake name overwrites all of the system arguments and file name to make it seem like a legitimate program.
- Automatically Daemonizes

- Tries to set GUID/UID to 0 (root)

Windows Features:

- Hides Console Window
- Stub Size of around 700kb

Installation

To install the dependencies needed for the python generation script run.

```
pip3 install -r requirements.txt
```

Make sure to edit config.h and replace the provided domain with yours, you can change the fake name as well as the password.

To create a Linux binary:

Run the compile.sh script, this will create a file called binary in the bin folder.

To Create a Windows Binary:

This project was built using VS 2019, if you open the sln file using VS2019 select the release build and build it.

Usage

Run payload_manager.py with python3 to create a hex encoded payload, then update or create a txt record for your domain, make sure that the **TTL is set to 300 seconds!!!**

Payload Manager Usage:

```
$ ./payload_manager.py -h
@@@@@@@   @@@@@@@    @@@@@@    @@@@@@   @@@@@@@
@@@@@@@@  @@@@@@@@  @@@@@@@@  @@@@@@@@  @@@@@@@@
@@!  @@@  @@!  @@@  @@!  @@@  @@!  @@@  @@!  @@@
!@!  @!@  !@!  @!@  !@!  @!@  !@!  @!@  !@!  @!@
@!@  !@!  @!@  !@!  @!@  !@!  @!@  !@!  @!@!!@!
!@!  !!!  !@!  !!!  !@!  !!!  !@!  !!!  !!@!@!
!!:  !!!  !!:  !!!  !!:  !!!  !!:  !!!  !!: :!!
:!:  !:!  :!:  !:!  :!:  !:!  :!:  !:!  :!:  !:!
 :::: ::   :::: ::  ::::: ::  ::::: ::  ::   :::
:: :  :   :: :  :    : :  :    : :  :    :   : :
usage: payload_manager.py [-h] [-l LINUX_CMD] [-w WINDOWS_CMD]
                          [-d DOMAIN_SEARCH]

ddoor, crossplatform dns backdoor

optional arguments:
  -h, --help        show this help message and exit
  -l LINUX_CMD      Linux Command
  -w WINDOWS_CMD    Windows Command
  -d DOMAIN_SEARCH  Domain to Check Commands On
```