ATTACK DEFENSE

by PentesterAcademy

Name	T1483: Domain Generation Algorithms
URL	https://www.attackdefense.com/challengedetails?cid=1578
Type	MITRE ATT&CK Linux : Command and Control

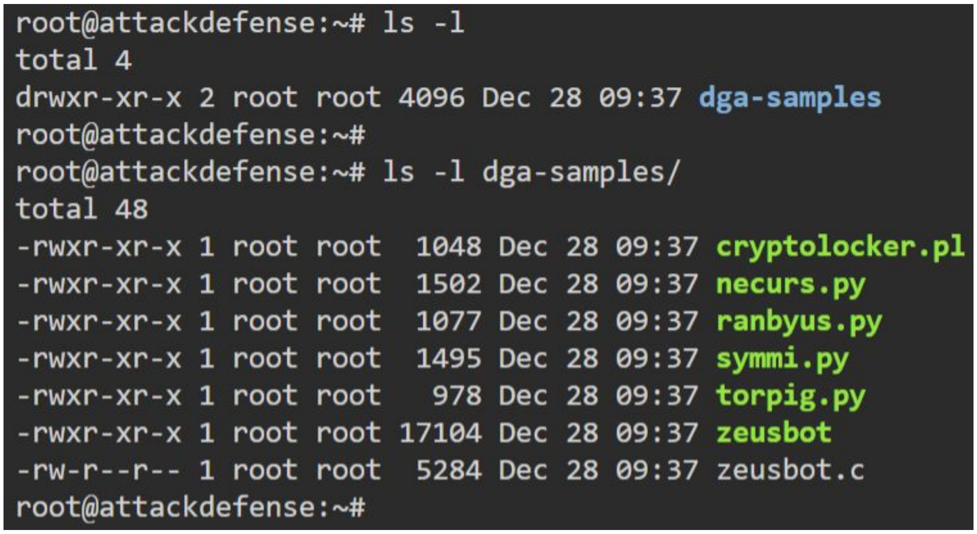
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Check and run different programs to understand how DGAs work!

Solution:

Step 1: Check the contents of the directory kept in the home directory of the root user.

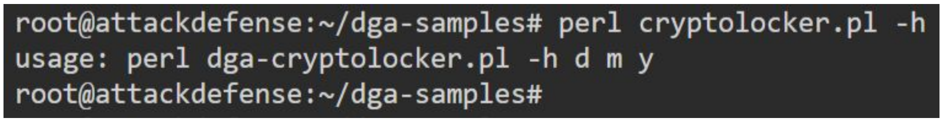
Commands:
ls -l
ls -l dga-samples



```
root@attackdefense:~# ls -l
total 4
drwxr-xr-x 2 root root 4096 Dec 28 09:37 dga-samples
root@attackdefense:~#
root@attackdefense:~# ls -l dga-samples/
total 48
-rwxr-xr-x 1 root root  1048 Dec 28 09:37 cryptolocker.pl
-rwxr-xr-x 1 root root  1502 Dec 28 09:37 necurs.py
-rwxr-xr-x 1 root root  1077 Dec 28 09:37 ranbyus.py
-rwxr-xr-x 1 root root  1495 Dec 28 09:37 symmi.py
-rwxr-xr-x 1 root root   978 Dec 28 09:37 torpig.py
-rwxr-xr-x 1 root root 17104 Dec 28 09:37 zeusbot
-rw-r--r-- 1 root root  5284 Dec 28 09:37 zeusbot.c
root@attackdefense:~#
```

Step 2: Check the arguments supported by cryptolocker.pl perl script.

Command: perl cryptolocker.pl -h

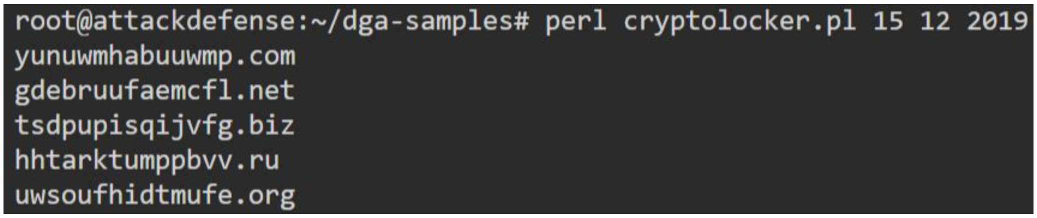


```
root@attackdefense:~/dga-samples# perl cryptolocker.pl -h
usage: perl dga-cryptolocker.pl -h d m y
root@attackdefense:~/dga-samples#
```

The script takes <day> <month> <year> as input.

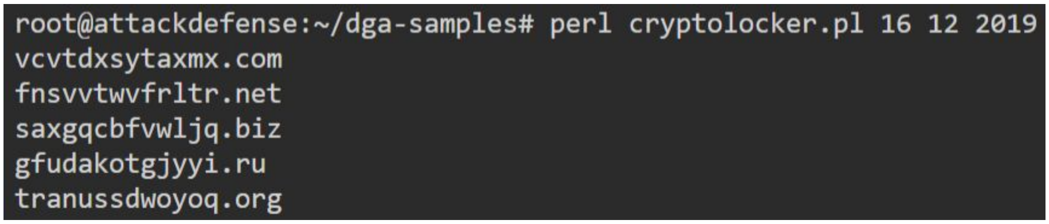
Observe the difference by running the script with date 15-Dec-2019 and 16-Dec-2019.

Command: perl cryptolocker.pl 15 12 2019



```
root@attackdefense:~/dga-samples# perl cryptolocker.pl 15 12 2019
yunuwmhabuuwmp.com
gdebruufaemcfl.net
tsdpupisqijvfg.biz
hhtarktumppbvv.ru
uwsoufhidtmufe.org
```

Command: perl cryptolocker.pl 16 12 2019



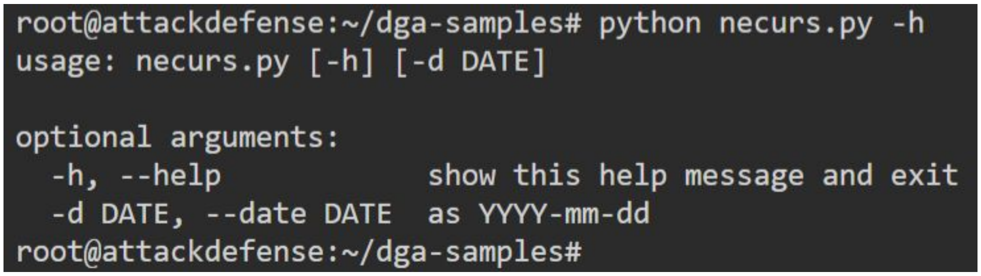
```
root@attackdefense:~/dga-samples# perl cryptolocker.pl 16 12 2019
vcvtdxsytaxmx.com
fnsvvtwvfrltr.net
saxgqcbfvwljq.biz
gfudakotgjyyi.ru
tranussdwoyoq.org
```

One can observe the difference in the domains generated for two consecutive days.

Note: The output (list of generated domains) is snipped here.

Step 3: Check the arguments supported by necurs.py python script.

Command: python necurs.py -h

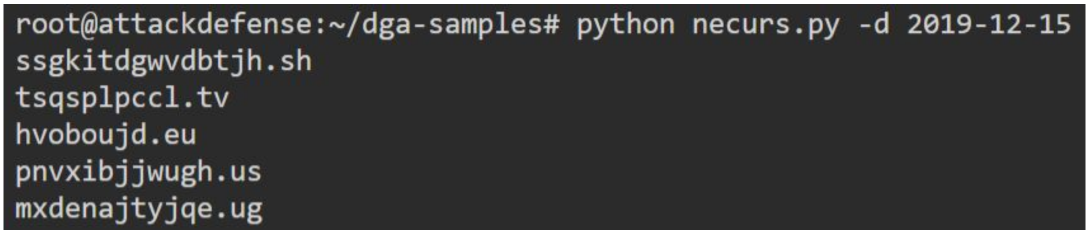


```
root@attackdefense:~/dga-samples# python necurs.py -h
usage: necurs.py [-h] [-d DATE]

optional arguments:
  -h, --help            show this help message and exit
  -d DATE, --date DATE  as YYYY-mm-dd
root@attackdefense:~/dga-samples#
```

The script takes YYYY-MM-DD as input.

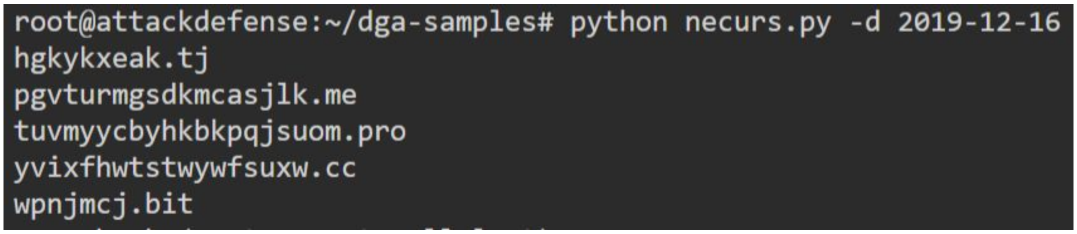
Observe the difference by running the script with date 15-Dec-2019 and 16-Dec-2019.

Command: python necurs.py 2019-12-15



```
root@attackdefense:~/dga-samples# python necurs.py -d 2019-12-15
ssgkitdgwvdbtjh.sh
tsqsplpccl.tv
hvoboujd.eu
pnvxibjjwugh.us
mxdenajtyjqe.ug
```

Command: python necurs.py 2019-12-16



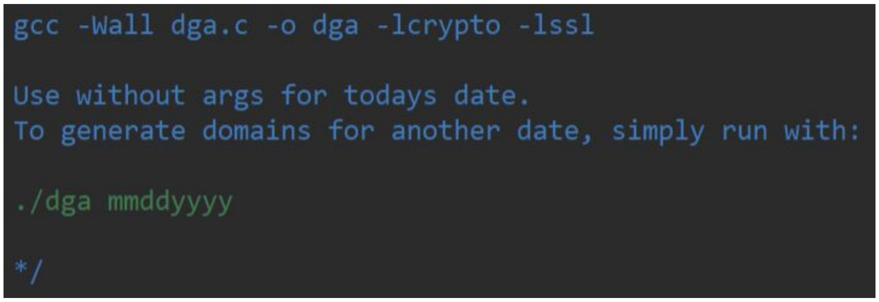
```
root@attackdefense:~/dga-samples# python necurs.py -d 2019-12-16
hgkykxeak.tj
pgvturmgsdkmcasjlk.me
tuvmyycbyhkbkpqjsuom.pro
yvixfhwtstwywfsuxw.cc
wpnjmcj.bit
```

One can observe the difference in the domains generated for two consecutive days.

In a similar manner, check the arguments for other python scripts and analyze/run them.

Step 4: Check the arguments supported by binary by checking its C code.

Command: vim zeusbot.c

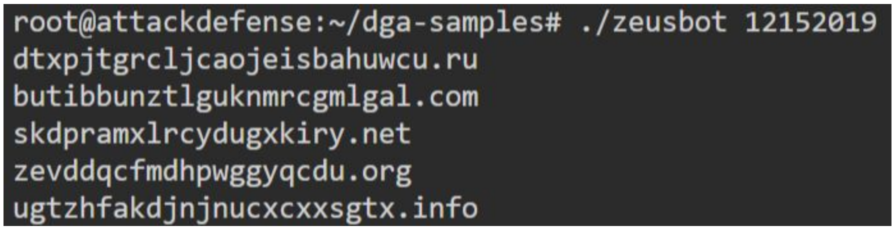


```
gcc -Wall dga.c -o dga -lcrypto -lssl

Use without args for todays date.
To generate domains for another date, simply run with:

./dga mmddyyyy

*/
```

The binary takes DDMMYYYY as input.

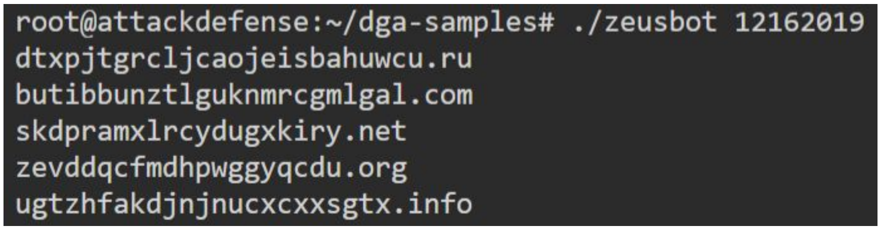
Observe the difference by running the script with date 15-Dec-2019 and 16-Dec-2019.

Command: ./zeusbot 12152019



```
root@attackdefense:~/dga-samples# ./zeusbot 12152019
dtxpjtgrcljcaojeisbahuwcu.ru
butibbunztlguknmrcgmlgal.com
skdpramxlrcydugxkiry.net
zevddqcfmdhpwggyqcdu.org
ugtzhfakdjnjnucxcxxsgtx.info
```

Command: ./zeusbot 12162019



```
root@attackdefense:~/dga-samples# ./zeusbot 12162019
dtxpjtgrcljcaojeisbahuwcu.ru
butibbunztlguknmrcgmlgal.com
skdpramxlrcydugxkiry.net
zevddqcfmdhpwggyqcdu.org
ugtzhfakdjnjnucxcxxsgtx.info
```

One can observe the difference in the domains generated for two consecutive days.

References:

- DGA Collection (https://github.com/pchaigno/dga-collection)