THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Computer Science 6907
Computer Network Defense

Homework #2

Kevin Yasuda
Matthew Norris

Maintaining Connections

As discussed in class, Domain Generation Algorithms (DGAs) are often implemented by malware authors as either a primary or secondary means of maintaining connectivity to their widely deployed bots. In the lecture, we provided samples of several mechanisms/algorithms that may be deployed to accomplish this.

For your homework assignment, develop a function in Python that will create a variable number of pseudorandom domains a day. A simple implementation is included below for reference - please develop your own algorithm and provide both the code that you created and at least a 250 word description of both how your algorithm works and why you chose it. Example wrapper code is provided to simplify your implementation. If you modify the wrapper code (e.g. to incorporate additional libraries), please include that in your description and submission.

```
def provide_generated_domain(date,iter):
        # create list of TLDs that will be chosen later
        tlds = ['com','net','org','ru','cn','tv']
        # create a hash of a string that is the date passed in and the iteration parameter
        string_to_hash = date + "-" + str(iter)
        hash = hashlib.md5()
        hash.update(string_to_hash)
        hashed_string = hash.hexdigest()
        # determine the final string length - from the number value of the first char (mod 10)
        length = ord(hashed_string[:1])%10 + 12
        # build the final domain
        #   hostname = the first 'length' characters of hash
        #   TLD = selected from tlds array by [first hashed character (mod 6)]
        return hashed_string[:length]+"."+tlds[ord(hashed_string[:1])%6]
```

```
mnorris$ python print_DGA_domains.py --date 20160106 --count 10
b3e8d8056ea5fc7f3e1b.org
56152cbaba9c222.tv
cd6cdf5fdfb42df51471d.ru
290948763fbd.org
050fb1f84197401e0c30.com
85330d88247be5d653.org
9d759e58a8a99ff44af.ru
6b18033a62834ac8.com
0dc2f913726b3a194886.com
```