Rootkit
User Guide

Eunsaem Lee

December 6th, 2022

Table of Contents

Purpose

A rootkit application with a command-and-control system that:

- provides attacker with a menu to control the victim program
- sets victim IP address
- sets process name for camouflage
- reads commands from the attacker
- executes the commands on the victim
- sends the command output to the attacker
- encrypts sending data using AES cipher with encryption key and salt value
- decrypts receiving data using AES cipher with encryption key and salt value
- reads from the keyboard and sends the data over a covert channel
- encrypts sending data using Caesar Cipher with a key value
- decrypts receiving data using Caesar Cipher with a key value
- saves received data and files locally
- generates log files
- transfers a file from the victim to the attacker
- watches a file for changes; when the file changes, transfers it to the attacker
- watches a directory for changes; when a file is created or modified in the directory, transfers it to the attacker

Installing

Obtaining

`git clone https://github.com/eunsaemy/rootkit`

Installing

Install cryptography, pycryptodome, pynput, setproctitle, and Scapy using the commands:

- `pip install cryptography`
- `pip install pycryptodome`
- `pip install pynput`
- `pip install setproctitle`
- `pip install scapy`

Running

```
To run attacker.py
     python server.py
To run victim.py:
     python victim.py
```

Examples

Install cryptography

```
C:\Users\saemy>pip install cryptography
Collecting cryptography
  Using cached cryptography-38.0.4-cp36-abi3-win_amd64.whl (2.4 MB)
Requirement already satisfied: cffi>=1.12 in c:\users\saemy\appdata\local\programs\python\python310\lib\site-packa
ges (from cryptography) (1.15.1)
Requirement already satisfied: pycparser in c:\users\saemy\appdata\local\programs\python\python310\lib\site-packag
es (from cffi>=1.12->cryptography) (2.21)
Installing collected packages: cryptography
Successfully installed cryptography-38.0.4
```

Install pycryptodome

```
C:\Users\saemy\Desktop\BCIT\BTech\Level7\COMP 8505\Assignment\ASG3\source>pip install pycryptodome
Collecting pycryptodome
  Downloading pycryptodome-3.15.0-cp35-abi3-win_amd64.whl (1.9 MB)
     ---------------------------------------- 1.9/1.9 MB 9.5 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.15.0
```

Install pynput

```
C:\Users\saemy\Desktop\ASG2>pip install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl (89 kB)
     ---------------------------------------- 89.2/89.2 kB 1.3 MB/s eta 0:00:00
Collecting six
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, pynput
Successfully installed pynput-1.7.6 six-1.16.0
```

Install setproctitle

```
C:\Users\saemy\Desktop\BCIT\BTech\Level7\COMP 8505\Assignment\ASG3\source>pip install setproctitle
Collecting setproctitle
  Downloading setproctitle-1.3.2-cp310-cp310-win_amd64.whl (11 kB)
Installing collected packages: setproctitle
Successfully installed setproctitle-1.3.2
```

Install Scapy

```
C:\Users\saemy\Desktop\BCIT\BTech\Level7\COMP 8505\Assignment\ASG3\source>pip install scapy
Collecting scapy
  Using cached scapy-2.4.5.tar.gz (1.1 MB)
  Preparing metadata (setup.py) ... done
Installing collected packages: scapy
  DEPRECATION: scapy is being installed using the legacy 'setup.py install' method, because
project.toml' and the 'wheel' package is not installed. pip 23.1 will enforce this behaviour
placement is to enable the '--use-pep517' option. Discussion can be found at https://github.
59
  Running setup.py install for scapy ... done
Successfully installed scapy-2.4.5
```

python attacker.py

```
01:21:05(-)root@localhost:Desktop$ python attacker.py
IP address of the victim:
```

```
01:21:05(-)root@localhost:Desktop$ python attacker.py
IP address of the victim: 192.168.0.23
Process name for deception (default=abc):

IP address: 192.168.0.23
Port: 43813
Process name: abc

   1. Start the keylogger
   2. Stop the keylogger
   3. Transfer a file from the victim to the attacker
   4. Start watching a file for changes
   5. Stop watching a file for changes
   6. Start watching a directory for changes
   7. Stop watching a directory for changes
   8. Run shell script
   9. Change victim IP and Port & Process name
   0. Quit

Please choose an option:
```

python victim.py

```
01:47:39(-)root@localhost:Desktop$ python victim.py
```