SSC Incident Analysis

Daniel Kouril
EGI CSIRT

Introduction

- “Infected” VMs available
  - SSH, over custom ports
- Analysis of infections used during SSC
- Focus on general system investigations
  - No batch system or EGI specifics involved
- Several stages of the investigation

Stage 1
Triage

- Goals
  - Examine the system
  - Use commands `ps`, `lsof`, `netstat`,
  - Possibly check relevant records in `/proc/`

Stage 1
Triage

- Goals
  - Examine the system
  - Use commands `ps`, `lsof`, `netstat`,
  - Possibly check relevant records in `/proc/`
- Findings
  - Tor client/proxy running, active connections
  - Deleted executables used
- Summary – we probably have an incident
  - Snapshots, …

ps auxf

```
lhcbpil+ 26424  0.0  1.8  59496 34508 ?        Rs   Apr30   1:18 Browser/TorBrowser/Tor/tor
lhcbpil+ 10034  0.0  0.0 113180  1580 ?        S    12:41   0:00 /bin/sh ./dd07998c-dd7f-45bd-8585-82ce0397ff0a
lhcbpil+ 10091  0.0  0.0 115304  1672 ?        S    12:41   0:00  \_ /bin/bash ./dd07998c-dd7f-45bd-8585-82ce039
lhcbpil+ 10101  0.0  0.0   3152   828 ?        Ss   12:41   0:00     \_ ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.el
lhcbpil+ 10104  0.0  0.0  11684  1380 ?        S    12:41   0:00        \_ /bin/bash
```

netstat -tnp

```
tcp        0      0 78.128.250.235:54692    145.239.6.188:9001      ESTABLISHED 26424/Browser/TorBr
tcp        0     40 78.128.250.235:22       85.71.6.76:52760        ESTABLISHED 10499/sshd: root@pt
tcp        0      0 127.0.0.1:53568         127.0.0.1:9050          CLOSE_WAIT  10091/bash
tcp        0      0 127.0.0.1:9050          127.0.0.1:53570         ESTABLISHED 26424/Browser/TorBr
tcp        0      0 127.0.0.1:53570         127.0.0.1:9050          ESTABLISHED 10101/./dd07998c-dd
```

ls /proc/10101/exe (or lsof –p 10101)

```
lrwxrwxrwx. 1 root root 0 May  5 12:41 exe ->
                /home/lhcbpil01/dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf (deleted)
```

Stage 2
Live analysis, collecting evidence

- Goals
  - Collect information found during triage
    - Hierarchy of suspicious processes
    - Detect resources used by them
    - Detect deleted files in use and recover them
    - Obtain memory dumps of the processes
  - Stop activities

lsof -p 10034 -n
dd07998c- 10034 lhcbpil01 txt REG 253,1 964608 12602939 /usr/bin/bash
dd07998c- 10034 lhcbpil01 255r REG 253,1 437322 4389285 /home/lhcbpil01/dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin (deleted)

lsof -p 10091 -n
dd07998c- 10091 lhcbpil01 txt REG 253,1 964608 12602939 /usr/bin/bash
dd07998c- 10091 lhcbpil01 9u IPv4 325793 0t0 TCP 127.0.0.1:53568->127.0.0.1:versiera (CLOSE_WAIT)
dd07998c- 10091 lhcbpil01 255r REG 253,1 1108 8456425 /home/lhcbpil01/dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh (deleted)

lsof -p 10101 -n
a7nCrD 10101 lhcbpil01 txt REG 253,1 335408 8456445 /home/lhcbpil01/dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf (deleted)
a7nCrD 10101 lhcbpil01 3u IPv4 325798 0t0 TCP 127.0.0.1:53570->127.0.0.1:versiera (ESTABLISHED)
a7nCrD 10101 lhcbpil01 9u IPv4 325793 0t0 TCP 127.0.0.1:53568->127.0.0.1:versiera (CLOSE_WAIT)

lsof -p 10104 -n
bash 10104 lhcbpil01 txt REG 253,1 964608 12602939 /usr/bin/bash
bash 10104 lhcbpil01 0u IPv4 325798 0t0 TCP 127.0.0.1:53570->127.0.0.1:versiera (ESTABLISHED)
bash 10104 lhcbpil01 1u IPv4 325798 0t0 TCP 127.0.0.1:53570->127.0.0.1:versiera (ESTABLISHED)
bash 10104 lhcbpil01 2u IPv4 325798 0t0 TCP 127.0.0.1:53570->127.0.0.1:versiera (ESTABLISHED)
bash 10104 lhcbpil01 3u IPv4 325798 0t0 TCP 127.0.0.1:53570->127.0.0.1:versiera (ESTABLISHED)
bash 10104 lhcbpil01 9u IPv4 325793 0t0 TCP 127.0.0.1:53568->127.0.0.1:versiera (CLOSE_WAIT)

lsof -p 26424 -n
tor 26424 lhcbpil01 cwd DIR 253,1 6 4389281 /home/lhcbpil01/tor-browser_en-US (deleted)
tor 26424 lhcbpil01 rtd DIR 253,1 224 64 /
tor 26424 lhcbpil01 txt REG 253,1 3102224 1894387 /home/lhcbpil01/tor-browser_en-US/Browser/TorBrowser/Tor/tor (deleted)
tor 26424 lhcbpil01 mem REG 253,1 3727121 12606433 /home/lhcbpil01/.tor/cached-microdescs
tor 26424 lhcbpil01 6u IPv4 61890 0t0 TCP 127.0.0.1:versiera (LISTEN)
tor 26424 lhcbpil01 8u IPv4 325799 0t0 TCP 127.0.0.1:versiera->127.0.0.1:53570 (ESTABLISHED)
tor 26424 lhcbpil01 12u IPv4 325803 0t0 TCP 78.128.250.235:54692->145.239.6.188:etlservicemgr (ESTABLISHED)

- mkdir /dev/shm/evidence

- mkdir $PID
- cd /proc/$PID
- ls -l {exe,cwd,fd}
- cp exe /dev/shm/evidence/$PID/NAME
- cp fd/$FD /dev/shm/evidence/$PID/NAME

- cd /dev/shm/evidence
- for i in *; do gcore -o $i/gcore $i; done

10101/gcore.10101
10101/dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf

26424/gcore.26424
26424/tor

10034/gcore.10034
10034/dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin

10091/dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh
10091/gcore.10091
10104/gcore.10104

for i in *; do kill -STOP $i ;done

```
lhcbpil+ 26424  0.0  1.8  60532 35508 ?        Ts   Apr30   1:19 Browser/TorBrowser/Tor/tor
lhcbpil+ 10034  0.0  0.0 113180  1600 ?        T    12:41   0:00 /bin/sh ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin
lhcbpil+ 10091  0.0  0.0 115304  1692 ?        T    12:41   0:00  \_ /bin/bash ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh
lhcbpil+ 10101  0.0  0.0   3152   828 ?        Ts   12:41   0:00      \_ ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf
lhcbpil+ 10104  0.0  0.0  11684  1404 ?        T    12:41   0:00        \_ /bin/bash
```

Stage 3
File analysis

- Goals
  - Review memory dumps
    - Bash processes
    - Bots
  - Review files/executables recovered
    - Script
    - Binary
- In real world the analysis is done elsewhere!

Recovered files

- dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin
- dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh
- dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf

dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin

- Self-extractable shell-script – unpacks and executes the payload (and deletes it after start)
  - Edit the script:
    - keep=y
    - verbose=y
- [user@m]$ ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.bin

  Verifying archive integrity... All good.

  About to extract 424 KB in . ... Proceed ? [Y/n]

  Uncompressing dd07998c-dd7f-45bd-8585-82ce0397ff0a.....

  OK to execute: ./dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh ? [Y/n] n

  /bin/rm: refusing to remove ‘.’ or ‘..’ directory: skipping ‘.’
- Be aware that you run an attacker’s commands

Analysis of *.bin

-rwxr-xr-x. 1 user user 335408 Jan 1 1970 dd07998c-dd7f-45bd-8585-82ce0397ff0a.elf

-rwxr-xr-x. 1 user user 1108 Jan 1 1970 dd07998c-dd7f-45bd-8585-82ce0397ff0a.sh

-rwxr-xr-x. 1 user user 365 Jan 1 1970 download-tor.sh

-rw-r--r--. 1 user user 26433 Jan 1 1970 tor32.torrent

-rw-r--r--. 1 user user 25953 Jan 1 1970 tor64.torrent

-rwxr-xr-x. 1 user user 26433 Jan 1 1970 tor.torrent

- Some recovered file match to other recovered files
- *.sh is the entry point

Analysis of *.sh

- A simple shell script
- Deploys the malware and activates it
- If not done, it deploys Tor client
- Starts the bot (*.elf) and deletes files

Analysis of *.elf

- `ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped`
- `strings` doesn't reveal anything but UPX-related info
- `upx –d binary`
- `strings` more verbose now:
  - a static binary

Analysis of *.elf

- `ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped`
- `strings` doesn't reveal anything but UPX-related info
- `upx –d binary`
- `strings` more verbose now:
  - `FLAG GOEH`
  - `S HERE PH`
  - `AY ATTENH`
  - `TIONH`
  - `9050`
  - `127.0.0.1`
  - `egisscjvgjwp5dqv.onion`
  - `/bin/bash`
  - `4bb02f8c-be15-407f-a573-58921de72969`
  - `WELCOME TO THE PARTY`

Memory analysis

- Memory dump of *.elf
  - Strings visible from binary
  - A flag mentioned
- Check the dump of the last bash process
  - Should contain commands received from C&C

Memory analysis

- *.elf
  - Strings visible from binary
  - A flag mentioned
    - 4bb02f8c-be15-407f-a573-58921de72969
    - 4bb02f8c-be15-407f-a573-5-407f-a573-5892
      - the latter one is only kept in memory
- Check the dump of the last bash process
  - Should contain commands received from C&C
    - ps aux | grep yes
    - /dev/null &
    - grep yes
    - sid yes > /dev/null
    - /usr/bin/id
    - /usr/bin/hostname
    - /usr/bin/whoami
    - nohup setsid yes > /dev/null