Hands-on Exercises

Starting investigation

- SOC-raised alert about suspicious communication
  - Communication using *Stratum* protocol was detected
  - The destination was ap.luckpool.net, port 3956/tcp
  - The source was your machine
    - The machine is a small server, used only for internal purposes of your organisation

Task 1

Check the system and find anything suspicious

Findings

- Suspicious network connection
- Connection originates from a root-owned process

- Trigger incident response procedure now

- Forensics acquisition
  - Snapshot the machine, if possible
  - Get metadata from filesystem before other steps
  - Keep the process running or not? (`kill -STOP PID`)

Checking Process

- Allocated resources/metadata
  - `ps ax | grep crond`
  - `lsof -p 2584`
- Always try to correlate multiple sources/commands
  - `/proc/PID/exe`
  - `/proc/PID/fd`
  - `/proc/PID/cwd`

Task 2

Check binary /usr/sbin/crond and try to estimate its purpose or other details.

Findings

- A compiled binary (C-code), stripped, no obvious obfuscations
  - Likely an HTTP client (CURL-based)
  - Couple of other system/library calls visible
  - Control server URL embedded and visible

- Obvious payload management:
  - `Payload dropped to: %s`
  - `Payload started`

Process analysis

- The program is likely a dropper downloading payload from the master and executing it on the machine

- Can we find out more about the payload shipped?

Task 3

Check the memory dump produced by gcore and try to find additional traces about the dropping phase. Can you identify the file that was dropped on the system recently?

(Memory dump can be acquitted using `gcore PID`)

Findings

- Internal log:
  - `Payload dropped to: /usr/sbin/rsyslogd-worker`
  - `Payload started`

Task 4

Analyse rsyslogd-worker and detect interesting files that the process is using and examine the file.

Findings

- A deleted file in use
  - `/usr/lib/x86_64-linux-gnu/libcron.so.1`
  - `cp /proc/PID/fd/3 /dev/shm/3`
- Mining activities confirmed
- Another malicious IP detected

Part two