Lab 3. Windows Incident Response: Forensic Investigation and System Recovery

1. Prepare the machine.

Enable prefetch files for all applications

Here you can read what are prefetch files and why they are an important resource for a forensic investigation.

Use registry editor and navigate to the following key

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
```

Set `EnablePrefetcher` and `EnableSuperfetch` values to `0x3`. If not present, just add them.

Enable advanced logging using sysmon.

Sysmon (System Monitor) is an advanced logging service for Windows based systems.
All the information about its configuration is present in the download page provided above.
For a more high-quality event tracing, here is a configuration file template.
You can use the default sysmon's settings, the provided config file or a modified version. It's up to you, but a well structured config file can avoid generation of irrelevant logs and make your analysis process easier.

2. Run the malware.

Let it some time to do its job. Just leave the machine running and go to the next steps.

3. Extract and analyze the memdump.

Use the following command to get the uuid of the machine

```
VBoxManage list vms
```

Extract the memory dump using the dumpvmcore command:

```
VBoxManage debugvm <uuid> dumpvmcore --filename=<your-file-name>.elf
```

Now you can save the machine state.

Analysis will be done using the volatility3 tool. Refer to the README file for installation instructions.

Here you can find the documentation for v3 modules, and here for v2 (some of them were renamed, but are still relevant also for v3).

What can you obtain from a memdump:

1. Running processes;
2. Process hierarchy;
3. Process startup location;
4. Active connections;
5. Open handles;
6. Prefetch files.

Relevant modules: psscan, pslist, pstree, cmdline, malfind, netscan, handles.

4. Create a disk dump and analyze it.

Find the uuid of the last snapshot of the machine

```
VBoxManage list hdds
```

Merge the snapshots into the base image and obtain a raw version of the disk.

```
VBoxManage clonemedium <uuid> <nume-fisier>.dd --format=raw
```

Here you can find the docs for the provided commands.

Use Arsenal Image Mounter to mount the file for analysis.
As mount options, use `Disk device, write temporary` with in RAM storing. Also check `Create "removable" disk device`. The files will be accessible from Explorer as a removable disk.

First thing you can do is to look into the paths you found during the memdump analysis, like the location of some suspicious programs or open handles to files. The best that can happen is finding the actual malicious executable file, which can be further analyzed (this was already done is laboratory work 1).

Prefetch files analysis

To read them, you may use any tools, but here are some examples: PFCmd (cli) and WinPrefetchView (gui).

Hive analysis

Registry Explorer is an advanced tool for analyzing hive files. Compared to default registry editor, it has the option to find keys that were modified during a specified time period. It's very helpful when we know when the malware was run for the first time.

Autoruns entries

Use the Offline Analysis feature from Autoruns. As the root system, you should select the Windows folder of the mounted disk.

Event logs

Event logs in windows are stored in `X:\Windows\System32\winevt\Logs`. Sysmon logs are stored inside `Microsoft-Windows-Sysmon%4Operational.evtx` file. You can open them with the builtin Event Viewer or use FullEventLogView.

Here are some of the most relevant event IDs you should look for.

5. System Recovery

Try to clean up the system and remove all malware entries.