CS7038 - Malware Analysis - Wk09.2

Dynamic Analysis Tools

Coleman Kane
kaneca@mail.uc.edu

March 8, 2018

Overview

Sysmon: System activity logging system

Yara: Static analysis tool we've used in the past, but also capable of run-time analysis, both file & process memory scanning

FakeNet & inetsim: Network service simulators useful for simulating various services for malware to interact with

CaptureBAT: System monitor that can capture artifacts from filesystem changes.

Sysmon

Configurable system monitor, originally designed to assist developers by providing inspection into system-level events. With configuration, can be useful for monitoring and logging Windows host activity.

A helpful configuration to start from:
`https://github.com/SwiftOnSecurity/sysmon-config`

Utilizes the Event Tracing API for Windows:

`https://msdn.microsoft.com/en-us/library/windows/desktop/aa363795(v=vs.85).aspx`

In Windows Event Viewer, the SysMon event logs are accessible in the following compartment:

```
Applications and Services Logs/
->Microsoft/
->Windows/
->Sysmon/
->Operational
```

Sysmon Features

SysMon allows you to inspect and log the following event types:

- Process create/exit, Process-Process accesses
- File create time changes
- Thread creation
- File creation
- Pipe creation/connection
- WMI events
- Raw device access (\\.\)
- Driver load
- Image (EXE/DLL) load
- Network connections
- Registry events

Network Simulation

When working with malware, it often requires some sort of network access in order to function. Therefore, it can be advantageous to have a tool that can simulate network services for you. This is where the "Host-only Network" setting for VirtualBox truly shows its value.

DNS simulation is a common use-case. I typically use `dnsmasq` to accomplish this, as it allows me to write a simple configuration that can be used to make a DNS server listen on solely `vboxnet0`'s IP.

Two tools I recommend to use for this practice are **FakeNet-ng** and **inetsim**. These are Linux programs that can be executed either within your host environment, or from a secondary Linux VM.

Network Sim.: dnsmasq

The `dnsmasq` tool: `http://www.thekelleys.org.uk/dnsmasq/doc.html`.

Using a fairly simple configuration you can run this service as a DNS server, on your host, dedicated to serving your VMs. Alternately, by changing `vboxnet0` into `eth0` you can run it inside of a Linux VM on the same Host-only or Internal Network.

Example configuration:

```
interface=vboxnet0
address=/#/192.168.56.1
no-resolv
bind-interfaces
no-dhcp-interface=vboxnet0
```

Network Sim.: inetsim

An Open-Source tool, Internet Services Simulation Suite (inetsim): `http://www.inetsim.org/`. This tool provides the ability for you to simulate numerous popular services that may represent network protocols used by a malware sample.

Services supported

- HTTP/HTTPS
- Mail protocols (SMTP/POP)
- IRC
- Common UNIX services

Network Sim.: FakeNet-ng

An open-source tool that was developed by FireEye and is incorporated into some of its commercial tools. Has some of the service simulations as inetsim, but also offers some proxy functionality.

- `https://www.fireeye.com/blog/threat-research/2016/08/fakenet-ng_next_gen.html`
- `https://github.com/fireeye/flare-fakenet-ng`

Host monitoring: CaptureBAT

A host-monitoring tool, designed for Windows, that inspects system effects on the filesystem, process, thread, network, and registry levels. A helpful feature of this tool is that it can interrupt *file deletion* tasks in order to recover a copy of the file prior to deletion. Forensically, this can be very helpful for multi-stage attacks, such as the one depicted in the prior lectures.

More information:

- https://www.honeynet.org/node/315
- http://dfrws.org/sites/default/files/session-files/paper-capture_-_a_tool_for_behavioral_analysis_of_applications_and_documents.pdf