Hook Analyser

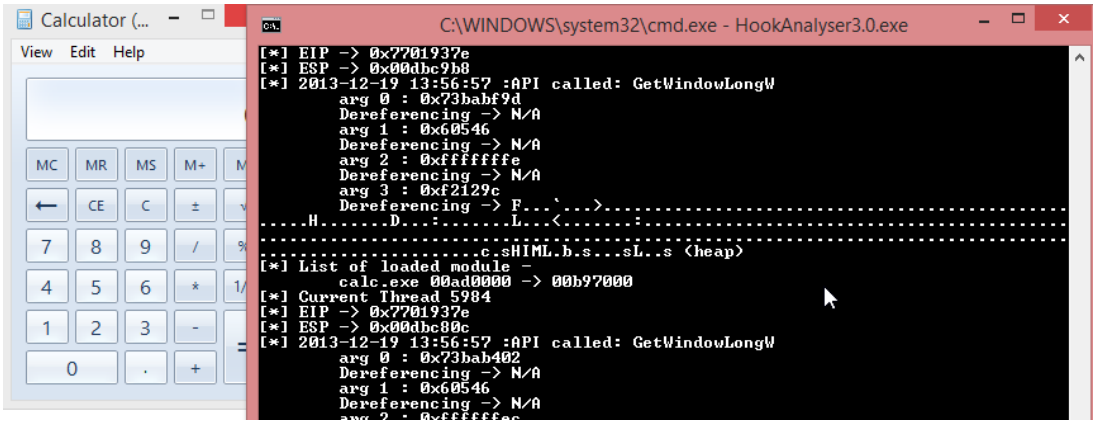
Hook Analyser is a malware analysis and cyber intelligence (gathering and analysis) utility.

The project/utility has six (6) key functionalities -

1. **Spawn and Hook to Application** - This feature allows analyst to spawn an application, and hook into it. The module performs the following -
    a. PE validation
    b. Static malware analysis.
    c. Other options (such as pattern search or dump all)
    d. Type of hooking (Automatic, Smart or manual)
    e. Spawn and hook

    With the 'hook' module, there are three types of hooking being supported –

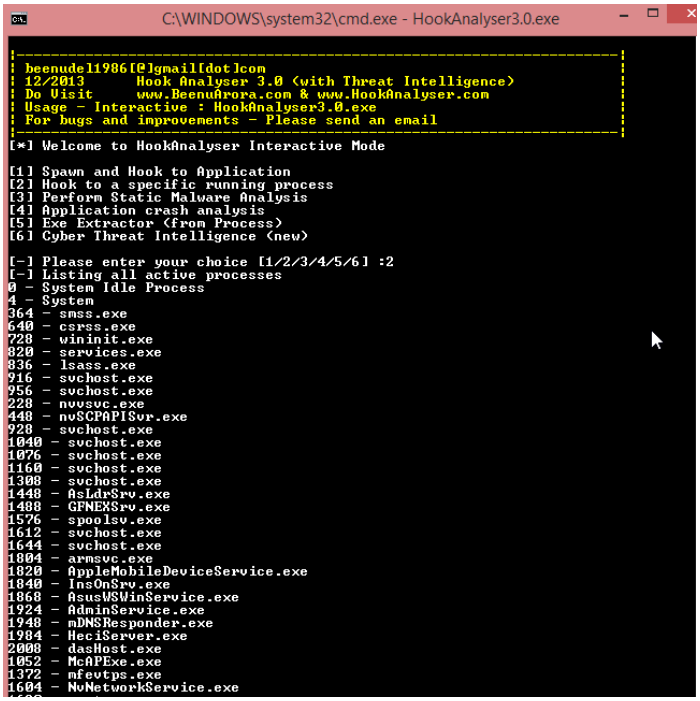
    a) Automatic – The tool will parse the application import tables, and based upon that will hook into specified APIs
    b) Manual – On this, the tool will ask end-user for each API, if it needs to be hooked.
    c) Smart – This is essentially a subset of automatic hooking however, excludes uninteresting APIs.



Spawn and Hook

2. **Hook to a specific running process**-The option allows analyst to hook to a running (active) process. The module performs the following operations –

    a. List all running process
    b. Identify the running process executable path.
    c. Perform static malware analysis on executable (fetched from process executable path)
    d. Other options (such as pattern search or dump all)
    e. Type of hooking (Automatic, Smart or manual)
    f. Hook to a specific running process
    g. Hook and continue the process



Hook to a Process

3. **Static Malware Analysis** - This module is one of the most interesting and useful module of Hook Analyser, which performs scanning on PE or Widows executables (and DLLs) to identify potential malware traces.

    a. PE file validation
    b. CRC and timestamps validation
    c. PE properties such as Image Base, Entry point, sections, subsystem
    d. TLS entry detection.
    e. Entry point verification (if falls in suspicious section)
    f. Suspicious entry point detection
    g. Packer detection

h. Signature trace (extended from malware analyser project), such as Anti VM aware, debug aware, keyboard hook aware etc. This particular function searches for more than 20 unique malware behaviours (using 100's of signature).
i. Import Intel scanning.
j. Deep search (module)
k. Online search of MD5 (of executable) on Threat Expert.
l. String dump (ASCII)
m. Executable file information
n. Hexdump
o. PEfile info dumping
p. ...and more.

Static Analysis

4. **Application crash analysis** - This module enables exploit researcher and/or application developer to analyse memory content when an application crashes. This module essentially displays data in different memory register (such as EIP).

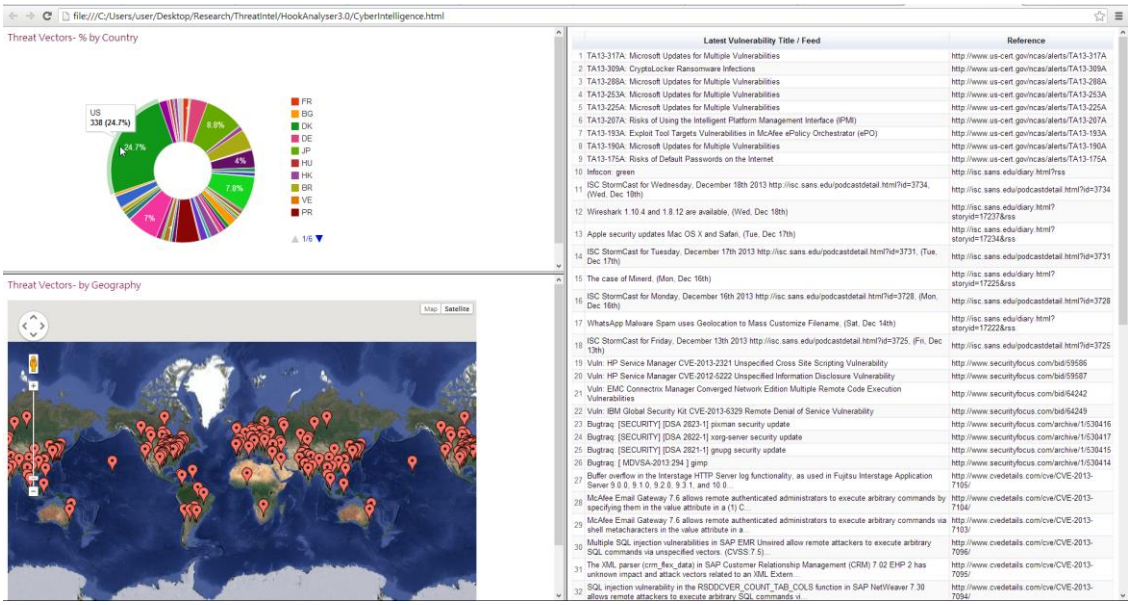
    - Application crash analysis video demonstration – http://www.youtube.com/watch?v=msYo7pPsu6A

5. **Exe extractor** - This module essentially extracts executables from running process/s, which could then be further analysed using Hook Analyser, Malware Analyser or other solutions. This module is potentially useful for incident responders

6. **Cyber Threat Intelligence** - This module is being created to gather and analyse information related to Cyber Threats and vulnerabilities. The module can be run using HookAnalyser.exe (via Option 6), or can be run directly.

   The module present information on a web browser (with dashboard alike representation). It has three (3) presentations -

   - Threat Vectors - by Country (through url.txt - provided)
   - Threat Vectors - by Geography (through url.txt - provided)
   - Vulnerability / Threat Feed (through rss.txt)



Cyber Threat Intelligence