

# Hook Analyser

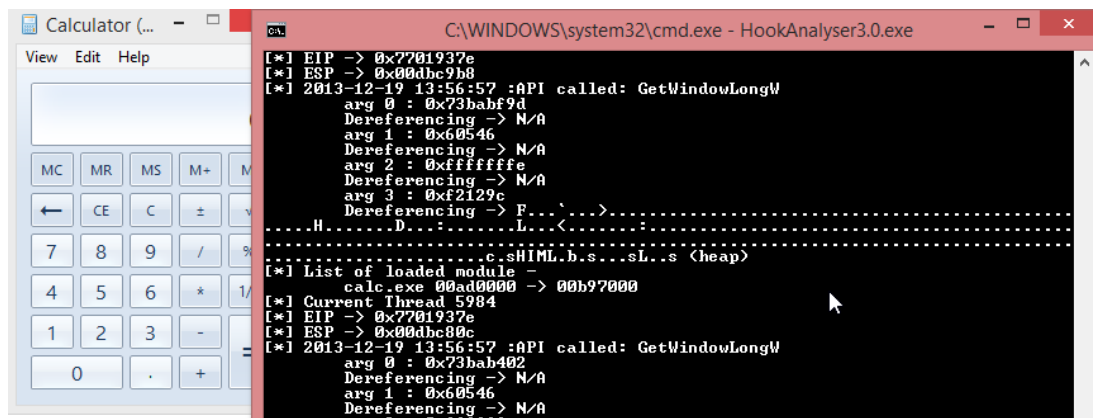
Hook Analyser is a malware analysis and cyber intelligence (gathering and analysis) utility.

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

```

C:\WINDOWS\system32\cmd.exe - HookAnalyser3.0.exe

[BeenuDel1986@gmail.com]
12/2013 Hook Analyser 3.0 (with Threat Intelligence)
Do Visit: www.BeenuDel1986.com & www.HookAnalyser.com
Usage - Interactive : HookAnalyser3.0.exe
For bugs and improvements - Please send an email

[*] Welcome to HookAnalyser Interactive Mode

[1] Spawn and Hook to Application
[2] Hook to a specific running process
[3] Perform Static Malware Analysis
[4] Application crash analysis
[5] Exe Extractor (from Process)
[6] Cyber Threat Intelligence (new)

[-] Please enter your choice [1/2/3/4/5/6] :2
[-] Listing all active processes
0 - System Idle Process
4 - System
364 - smss.exe
640 - csrss.exe
720 - wininit.exe
820 - services.exe
836 - lsass.exe
916 - svchost.exe
956 - svchost.exe
220 - nvsvc.exe
448 - nvSCPAPISrv.exe
920 - svchost.exe
1040 - svchost.exe
1076 - svchost.exe
1160 - svchost.exe
1308 - svchost.exe
1448 - AsLdrSrv.exe
1488 - GFNEXSrv.exe
1576 - spoolsv.exe
1612 - svchost.exe
1644 - svchost.exe
1804 - armsvc.exe
1820 - AppleMobileDeviceService.exe
1840 - InsOnSrv.exe
1860 - AsusVSMService.exe
1924 - AdminService.exe
1948 - mDNSResponder.exe
1984 - HeciServer.exe
2008 - dasHost.exe
1052 - MpExe.exe
1372 - mfeutps.exe
1604 - NuNetworkService.exe

```

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 Windows 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.

```

C:\WINDOWS\system32\cmd.exe

beenuro1986@sigmaildotcom
12/2013 Hook Analys3r 3.0 (with Threat Intelligence)
Do Visit www.beenuro1986.com & www.hookanalys3r.com
Usage : Interactive : HookAnalys3r3.0.exe
For bugs and improvements - Please send an email

[+] Welcome to HookAnalys3r Interactive Mode

[1] Spawn and Hook to Application
[2] Hook to a specific running process
[3] Perform Static Malware Analysis
[4] Application crash analysis
[5] Exe Extractor (from Process)
[6] Cyber Threat Intelligence (new)

[-] Please enter your choice [1/2/3/4/5/6] :3
[-] Enter the filename or filename with path :i.exe

[+] Digging the file
[+] Found exe at the offset 0x0
[+] Digging the file i.exe
[+] Something went wrong in digging module
[+] Analyzing if valid PE file
[+] Valid PE File
[+] File Size : 798 KB
[+] Verifying CRC from file
[+] CRC Seems fine
[+] Verifying timestamp from file
[+] Timestamp seems fine
[+] Compile time : [Thu Aug 22 03:29:39 2013 UTC]
[+] Image Base : 0x40000000
[+] Address Of Entry Point: 0x1B8D4L
[+] Number of RVA and Sizes: 16
[+] Subsystem: IMAGE_SUBSYSTEM_WINDOWS_GUI
[+] Searching for ILS entries..
[+] No ILS entries identified
[+] Found Entry Point at section: text
[+] Entry point in known section. Seems fine
[+] Executable seems to be packed using : [!] Executable seems to be packed using unknown packer
[+] Identifying Suspicious section
[+] Sections are suspicious
Section Name: IMAGE_SECTION_HEADER Entropy 7.54274909611
[+] [IMAGE_SECTION_HEADER]
0x258 0x8 Name: .PPE
0x260 0x8 Misc: 0x5D128
0x260 0x8 Misc PhysicalAddress: 0x5D128
0x260 0x8 Misc VirtualSize: 0x5D128
0x264 0xC VirtualAddress: 0x64000
0x268 0x10 SizeOfRawData: 0x5200
0x26C 0x14 PointerToRawData: 0x61000
0x270 0x10 PointerToRelocations: 0x0
0x274 0x10 PointerToLineNumbers: 0x0
0x278 0x20 NumberOfRelocations: 0x0
0x27C 0x20 NumberOfLineNumbers: 0x0
0x27C 0x24 Characteristics: 0x40000040

[+] Executable is Debug aware
[+] Executable is exception aware
[+] Executable can hook to keyboard
[+] Executable is potentially anti-debug aware
[-] Extracting file information from executable
LegalCopyright : Microsoft Corporation. All rights reserved.
InternalName : CALC
FileDescription : 6.3.9600.16384 (winblue_rtm.130821-1623)
CompanyName : Microsoft Corporation
ProductName : Microsoft Windows Operating System
ProductVersion : 6.3.9600.16384
FileDescription : Windows Calculator
OriginalFilename : CALC.EXE

[+] Performing deep search. There may be false positives, please verify manually
[+] Found 2 traces of Microsoft GDI control found
[+] Found 1591 traces of NOP instructions (a potential shellcode - Suspicious)
[+] Found 18 traces of potential filename
[+] Found 14 traces of potential NZ header
[+] Found 3 traces of potential VBN macros
[+] Found 10 traces of potential PE header

```

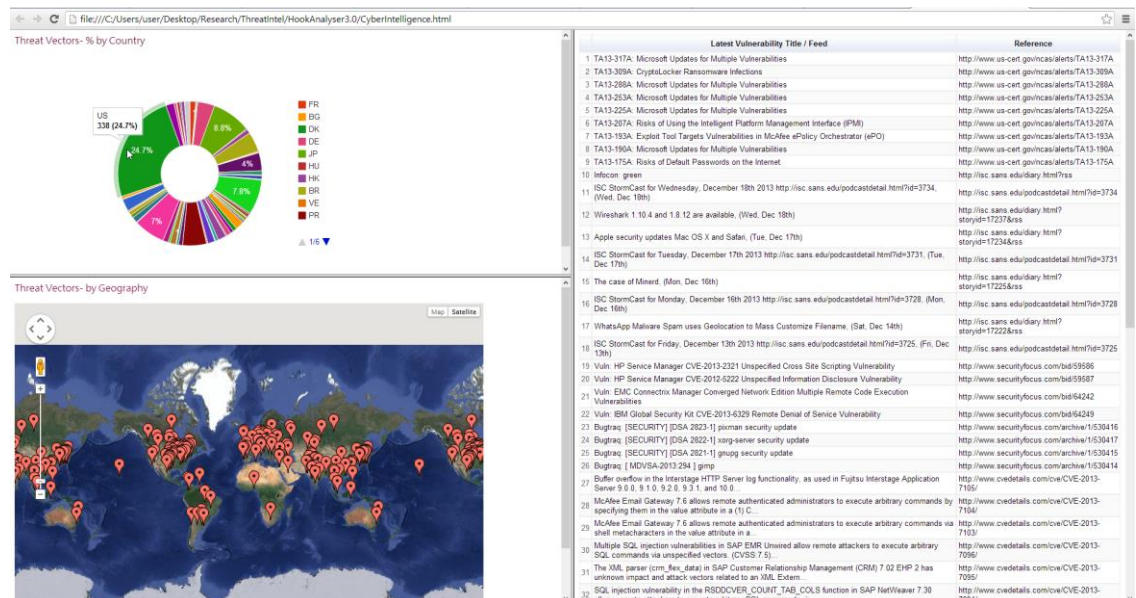
### Static Analysis

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