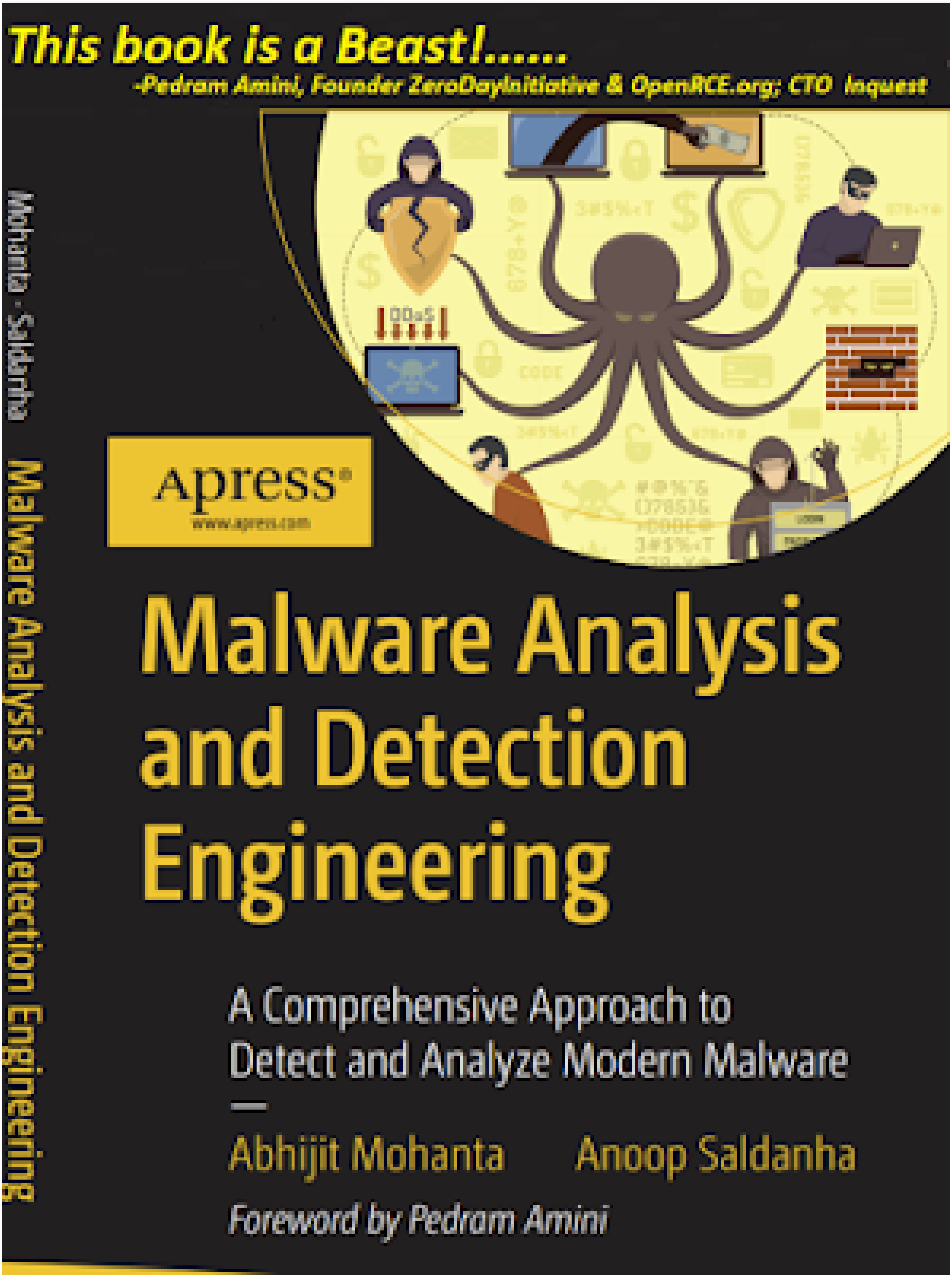
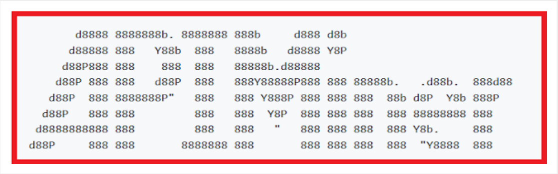

This book is a Beast!......
-Pedram Amini, Founder ZeroDayInitiative & OpenRCE.org; CTO Inquest
Apress®
www.apress.com
Malware Analysis and Detection Engineering
A Comprehensive Approach to Detect and Analyze Modern Malware
Abhijit Mohanta
Anoop Saldanha
Foreword by Pedram Amini
Mohanta · Saldanha
Malware Analysis and Detection Engineering

Home ▼

**Monday, 28 September 2020**

# APIMiner - The API Logger for Malwares - The Fast Way To Identifying Malwares



```
       d8888 8888888b. 8888888 888b     d888 d8b
      d88888 888   Y88b  888   8888b   d8888 Y8P
     d88P888 888    888  888   88888b.d88888
    d88P 888 888   d88P  888   888Y88888P888 888 88888b.   .d88b.  888d88
   d88P  888 8888888P"   888   888 Y888P 888 888 888  88b d8P  Y8b 888P
  d88P   888 888         888   888  Y8P  888 888 888  888 88888888 888
 d8888888888 888         888   888   "   888 888 888  888 Y8b.     888
d88P     888 888       8888888 888       888 888 888  888  "Y8888  888
```

**Direct Download Link for Latest Release of APIMiner:**
https://github.com/poona/APIMiner/releases/download/1.0.0/release-v1.0.0.zip

One of the biggest issues we have always faced is the availability of a stable API logger tool for Windows applications that can be used to analyze malware samples, that not only traces the Win32 APIs used by the parent process, but all its child processes as well. The real option that we have seen is Cuckoo Sandbox, but using Cuckoo Sandbox is unwieldy in a way, some of the reasons being,

1. Have seen enough people try to install Cuckoo Sandbox and fail at some step.
2. Practical deployments requires a separate Virtual Machine for installing and using Cuckoo Sandbox.
3. Unwieldy! As malware analysts and reverse engineer you don't want to waste time just to bring up a separate VM just to log APIs for a sample.

Now point (3) above is the most important one. As malware analysts I am pretty sure we already have our own Windows Analysis VMs which we have already setup with various tools. ***Why can't we run an API logger inside our existing Analysis VM? Why install another separate VM to generate API logs?*** This requirement became even more profound when we were writing our book **`Malware Analysis and Detection Engineering`** where we found the lack of any such tool stifling and we wanted to do something to drastically improve malware analysis and reversing speed.

And to solve all these issues we devised **APIMiner**. No extra VM required. Take your existing Malware Analysis VM, and run APIMiner from the command prompt to log APIs used by your malware sample. ***Super fast, easy and no complex setup!***

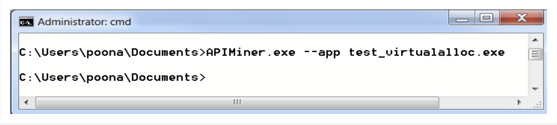
You can download the zip file for the latest release(release-v1.0.0) of APIMiner from **https://github.com/poona/APIMiner/releases**. The zip file from the release contains a README on how to install the tool and set it up. Currently it requires a config file **`apiminer_config.txt`**, but in a new release we will get rid of that and make things even more simpler. Also make sure you have added the `APIMiner.exe` to the **PATH** environment variable.

## Test Drive

*Enuf Talk!* Below is a simple sample C code which that does two things - allocates a memory chunk of *4096* bytes using `VirtualAlloc()` Win32 API and then changes the page permissions of this memory block using `VirtualProtect()` Win32 API.

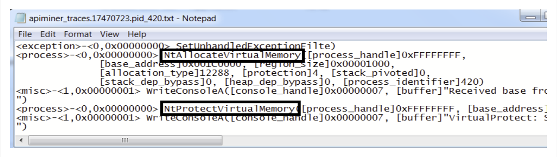
```
#include <stdio.h>
#include <stdlib.h>
#include <windows.h>

int main()
{
    void *addr;
    void *base;
    BOOL v;
    DWORD old;

    base = VirtualAlloc(NULL, 4096,
                        MEM_COMMIT | MEM_RESERVE,
                        PAGE_READWRITE);

    printf("Received base from VirtualAlloc: %x\n", base);

    v = VirtualProtect(base, 4096, PAGE_READONLY, &old);

    printf("VirtualProtect: %s\n",
           (v != 0) ? "Success" : "Failure");
    Sleep(1000000);
    return 0;
}
```

The above C code has been compiled into an executable `test_virtualalloc.exe` which we will now execute using *APIMiner* from the command prompt as seen below.



```
C:\Users\poona\Documents>APIMiner.exe --app test_virtualalloc.exe

C:\Users\poona\Documents>
```

Running the above command generates API log files having the `apiminer_traces` prefixes in their filenames in the *log folder* whose path you have specified in `apiminer_config.txt`. If you investigate these API trace files you will notice two APIs - `NtAllocateVirtualMemory` and `NtProtectVirtualMemory` which are the `NTAPI` variants of the APIS `VirtualAlloc` and `VirtualProtect` used by our above sample*. Fast and easy!*



```
<exception>-<0,0x00000000> SetUnhandledExceptionFilte)
<process>-<0,0x00000000> NtAllocateVirtualMemory([process_handle]0xFFFFFFFF,
                [base_address]0x001C0000, [region_size]0x00001000,
                [allocation_type]12288, [protection]4, [stack_pivoted]0,
                [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]420)
<misc>-<1,0x00000001> WriteConsoleA([console_handle]0x00000007, [buffer]"Received base fro
")
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]
<misc>-<1,0x00000001> WriteConsoleA([console_handle]0x00000007, [buffer]"VirtualProtect: S
")
```

Using APIMiner you can log the APIs used by any Windows executable. We have covered this tool extensively in our new book **Malware Analysis and Detection Engineering**, a 900+ comprehensive hands-on guide on Malware Analysis, Malware Reverse Engineering and Detection Engineering, published by *Apress* and available on the *Springer Network.* In this book we have explained various tricks that you can use in combination with our APIMiner tool to quickly analyze the behaviour of a sample and ascertain if it is a malware or not.

at September 28, 2020

Share

## 1 comment:

**Anonymous** 8 October 2020 at 19:58

Really good tool and thanks for making it free. I was always looking for something like this. I used to use Nttrace but it doesn't trace child processes. And the APIMonitor, but it is buggy and also is not free. Loving it so far. And the text file for API logs is great. I don't need any fancy processing to process the logs. And no more separate VM infra to run an API logger like the full Cuckoo setup. Loving it so far. Great job guys. And also ordered your book from Amazon. Looking forward to reading it.

Reply

Enter your comment...

Comment as: ashu.abviiitm@ Sign out

Publish Preview □ Notify me

Home ›

View web version

Powered by Blogger.