Kernel hacking tool you might have never heard of – XueTR/PCHunter

It is a good habit to keep your eyes open and monitor the updates to your favorite tools. I do it 'religiously' and comb the internet for the updates every once in a while. I know that some of these tools are never executed on my host machine, but they deliver an extremely unique and valuable interpretation of the system internals that I can act upon so I always want to have the latest, the best.

You definitely used Sysinternals tools, including the Process Explorer, and the Rootkit Revealer. You might have heard, or used GMER. Same for the RKU. Same for the Kernel Detective.

At least three of these tools were amazingly popular in the first decade of this century as they allowed to poke around things that other tools could only dream of. They were really ahead of a curve as they allowed to access the system in a nearly forensically-sound manner, unhook kernel and user mode hooks, scan the whole memory for badness and overall, really help to deal with a lot of nasty code from those days… One couldn't imagine a manual system repair of a system infected with a rootkit w/o one of these tools…

Now it's 2018, and Windows 10 is out there.

What tools can we use?

Most of the aforementioned tools are kaput.

There is some light though…

Enter Process Hacker
– a much better tool than Process Explorer.
I love Process Hacker and am really happy that it works on Win 10 pretty well.

While the official build is 2.39 and is 2 years old, there is a 'nightly' build you can always try to play with:

- https://wj32.org/processhacker/nightly.php

The last build, as of this post writing, is 3.0.1424 and is from 18/April/2018.

Yay! Go and get it!

Now… the one I want to talk about though is XueTR/PCHunter.

I bet you never heard of it.

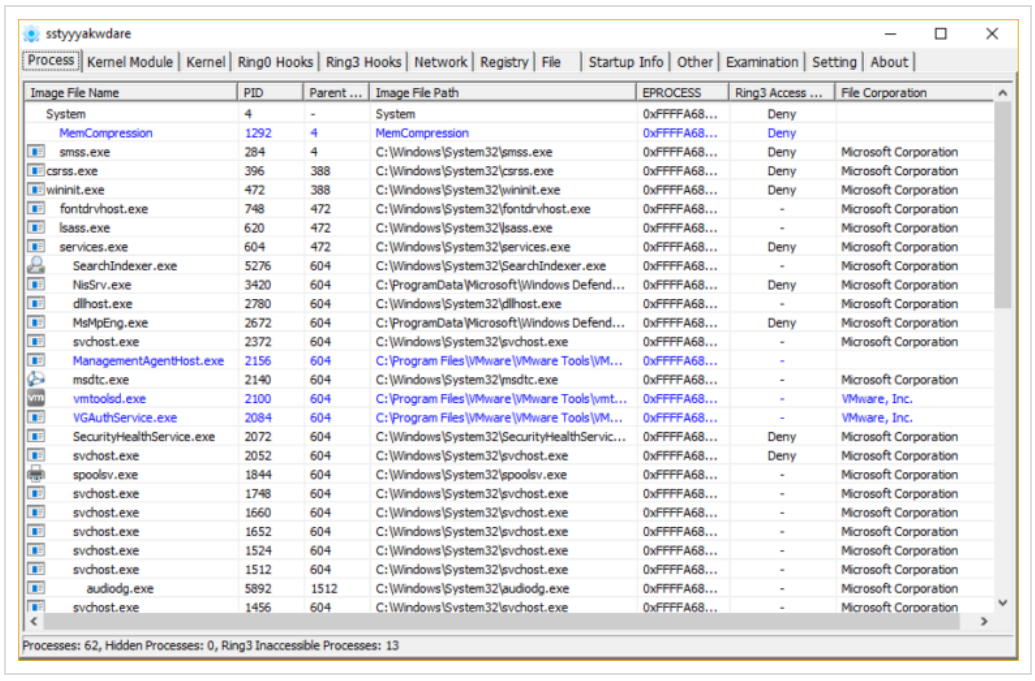
I have recently discovered that the author released a new version (in March 2018). The current version is 1.53 and according to the blog post it was tested with Win10 (16299).

Mind you. This is after 5 years of a hiatus on his blog, so this is great news that the author picked up and updated the tool.

Now… before we begin – please note that the free version of PcHunter works on 32- and 64- bit Windows 10, and can't be used commercially. This is explained in the About tab:

With that out of the way, we can explore the main interface.

When you execute the main 64-bit .exe (PCHunter64.exe) you will be presented with this UI:



The interface is (not a surprise) similar to GMER/RKU and to Kernel Detective.

There is a bunch of tabs we can browse through and which explore the Windows 10 internals in details:

- List of processes
- Kernel Modules
- Kernel 'Stuff'
  - Notify routines (e.g. these that notify the driver about a new process being created)
  - Filter
  - DPC Timer
  - Worker thread
  - Hal
  - Wdf
  - File System
  - System Debug
  - Object Hijack
  - Direct IO
  - GDT

- Ring0 Hooks (including IRP+inline)
  - SSDT
  - ShadowSSDT
  - FSD
  - Keyboard
  - I804prt
  - Mouse
  - Partmgr
  - Disk
  - Atapi
  - Acpi
  - Scsi
  - Kernel Hook
  - Object Type
  - IDT
- Ring3 Hooks
  - Message Hooks
  - Process Hook
  - KernelCallbackTable
- Network
  - Port
  - Tcpip
  - Nsiproxy
  - Tdx
  - Ndis Handler
  - IE Plugin
  - IE Shell
  - SPI
  - Hosts file
- Registry (browser)
- File (system browser)
- Startup Info
  - Startup
  - Services
  - Scheduled task
- Other
  - File Association
  - IFEO (Image File Execution Options)
  - IME/TIP
  - Firewall Rule
  - User Name
  - Other (additional tools)
- Examination (forensic-like report)
- Setting
- About

I am not going to include more screenshots. Download. Test. Make up your mind.

I think the tool is pretty cool and worth at least checking.

This entry was posted in **Reversing**, **Tips & Tricks** by **adam**. Bookmark the **permalink**.