

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Use Process Explorer to Identify Malware Infection](#)

Freebooter - September 24, 2015, 10:56 pm

[Process Explorer](#) is an advanced process management utility that picks up where Task Manager leaves off. It will show you detailed information about a process including its icon, command-line, full image path, memory statistics, user account, security attributes, and more. Process Explorer much better than Windows Task Manager it can help to identify malware infection on your system. Configure Process Explorer to detect malware infections. From "Options" menu select "Verify Image Signatures" if this is checked then images corresponding to processes are checked for trusted signatures automatically when you view a process properties and the result is shown next to the company field in the process properties dialog. "(Verified)" next a company name means the file is signed by a trusted root certificate authority and "(Unable to Verify)" means the file is either unsigned or signed by an untrusted authority. From "Options" menu click "VirusTotal.com" and place check marks on "Check VirusTotal.com" and "Submit Unknown Executables".

The information Process Explorer displays in its main window is fully configurable. You can reorder columns by dragging them to their new position. To select which columns of data you want visible in each of the views and the status bar, choose "View|Select Columns" or right-click on a column header and select "Select Columns" from the resulting context menu. A column selection editor opens that let's you pick the columns you want to enable, place a check mark on "Verified Signer" and "Virus Total" check boxes.

Thank You
?

GhostintheShock - September 25, 2015, 1:42 am

I followed your instructions and found this. I don't know if it is false alarm but if it is not than it is a matter of concern.

This is IDM(Internet download manager), latest version of this is installed. Then idmbroker.exe is scanned on virus total and found it is a worm.

[img]http://s27.postimg.org/je8t9wigx/idmbroker.png[/img]

Virus Total [Scan Report](#)

Decide it yourself.

Could be detected as it will start on startup.

Freebooter - September 25, 2015, 2:23 am

(Sep 25, 2015 01:42 AM)mikewaals Wrote: [\[CITE\]](#) I followed your instructions and found this. I don't know if it is false alarm but if it is not than it is a matter of concern.

This is IDM(Internet download manager), latest version of this is installed. Then idmbroker.exe is scanned on virus total and found it is a worm.

[img]http://s27.postimg.org/je8t9wigx/idmbroker.png[/img]

Virus Total [Scan Report](#)

Decide it yourself.

Could be detected as it will start on startup. One out of all malware scanner report idmBroker.exe as a worm infection as its known worm infection type few other malware scanners should be able to detect the idmBroker.exe as a worm as well i would say its false detection. The idmBroker.exe executable file is signed file, and signature has been verified.

freemium - September 25, 2015, 8:00 am

I just did it, nice tool thanks...

but dllhost.exe turn red sometime for no reason...can't open file, is this ok?

Freebooter - September 25, 2015, 9:31 am

(Sep 25, 2015 08:00 AM)freemium Wrote: [\[CITE\]](#)

I just did it, nice tool thanks...

but dllhost.exe turn red sometime for no reason...can't open file, is this ok? When a process exits, Process Explorer keeps it in the list for one second, highlighted in red. Note that even though the process appears in the list, if it is highlighted in red, the process has already exited and no longer exists. Which file you are not able to open.

freemium - September 25, 2015, 10:09 am

hmm odd

it keeps turning red all the time...

I mean green then red..green red at a few seconds interval and the pid keep changing

Freebooter - September 25, 2015, 11:27 am

(Sep 25, 2015 10:09 AM)freemium Wrote: [\[CITE\]](#)

hmm odd

it keeps turning red all the time...

I mean green then red..green red at a few seconds interval

and the pid keep changing No nothing strange in most cases you should never see DLLHOST.exe in Process Explorer, as typically DLLHOST.exe starts, does what it has to do, and then terminates.

Note: The dllhost.exe file is located in the C:\Windows\System32 and C:\windows\SysWOW64 folders. In other cases, dllhost.exe is a virus, spyware, trojan or worm!.

Visit URL link i posted to understand how to use Process Explorer.

"USING SYSINTERNALS TOOLS LIKE A PRO"

<http://www.howtogeek.com/school/sysinternals-pro/lesson2/>

freemium - September 26, 2015, 12:41 pm

thanks for the info, I should check it in depth ...

creki - September 26, 2015, 6:17 pm

I prefer process hacker, but thanks for sharing this info/tool ?

Freebooter - September 28, 2015, 7:43 am

(Sep 26, 2015 06:17 PM)Cracky. Wrote: [\[CITE\]](#) I prefer process hacker, but thanks for sharing this info/tool ? Thanks your very welcome. Process Hacker is better for debugging and reverse engineering, if you know how to use and setup Process Explorer its very powerful tool.

Phlox - July 7, 2017, 9:01 pm

"Malware Infection Removal and Security Tutorials"

<https://www.dost-tech.com/viewforum.php?f=18>

gzhat - July 7, 2017, 9:07 pm

(Jul 7, 2017 09:01 PM)Phlox Wrote: [\[CITE\]](#) "Malware Infection Removal and Security Tutorials" You guys have some pretty good tutorials i must say!

Phlox - July 9, 2017, 6:14 am

Thank you very much @gzhat!