

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Fast, free and easy way to check for system infections of FUD malware](#)

Forc?d - September 9, 2016, 10:43 am

As you hopefully know, most freshly spread malware are FUD. This makes it hard for Anti-Virus to detect infection. So i'm going to show you how to easily check for COMMON computer infections using freeware and your own brain :)

First of all your gonna need to download [Process Explorer](#)

This is one of many great internal tools from Microsoft, its basically a task-manager on steroids, with features such as direct hash checkup towards the VirusTotal database and signature checkup (Best feature)

You wanna run this and admin, it should look something like this.

This if a screenshot of its running a fresh VM infected by NanoCore.

Now you wanna go to Options>> And Check "Verify image signatures" also go to "VirusTotal.com" and check "Check VirusTotal"

This will cross check the hash of every running process with the Virus-total database, it will also check if the signature of the file is valid.

^And this is the important part, you can spoof and play with any file all you want, but only an authorized software publisher can assign file's a valid signature. This is basically the easiest way to check any file written to your disk may be possible malware or not.

But keep in mind, this applies only for the written exe/malware on disk, if a malware injects itself into another process, it will not change its valid signature. So this is to locate the physical written malware on disk.

As you can see this NanoCore stub has no valid signature and no HF crypter will be able to give it a valid one either. From here we can easily suspend the process , kill the process, locate the file and remove it.

The same applies for persistence, by suspending the process instead of killing it, your break most persistence by Trojans etc.

Microsoft also has another internal tool called "Autoruns", basically shows every startup reg key, so after you kill/suspend the process, you can remove their startup feature

Download: <https://technet.microsoft.com/en-us/sysinternals/bb963902>

Very good presentation for a more in-depth look, recommend for anyone dealing on HF.

https://www.youtube.com/watch?v=Wuy_Pm3KaV8

My English grammer < shit, PM me.

Anxious.exe - September 10, 2016, 4:58 am

Seems pretty cool, will give it a try soon.

yotoprules - September 10, 2016, 4:40 pm

Thanks a lot for this tutorial! I might give this a try if I or someone else ever gets infected

jimmyfer - September 10, 2016, 6:56 pm

Great tutorial, this is very usefull. Simple and excelent!

Anxious.exe - September 11, 2016, 1:08 am

Vouch for OP ! Amazing share, amazing tool.

Forc?d - September 11, 2016, 1:08 am

(Sep 10, 2016 04:58 AM)Anxious.exe Wrote: [\[CITE\]](#) Seems pretty cool, will give it a try soon.

(Sep 10, 2016 04:40 PM)yotoprules Wrote: [\[CITE\]](#) Thanks a lot for this tutorial! I might give this a try if I or someone else ever gets infected

(Sep 10, 2016 06:56 PM)jimmyfer Wrote: [\[CITE\]](#) Great tutorial, this is very usefull. Simple and excelent!

(Sep 11, 2016 01:08 AM)Anxious.exe Wrote: [\[CITE\]](#) Vouch for OP ! Amazing share, amazing tool. Glad you enjoyed

Forc?d - September 26, 2016, 7:04 am

I feel this can help allot of users out there, bumping.

warpje - September 26, 2016, 8:24 am

Learned something new nice tutorial! Will check the different RAT and crypter to see how it works with that!

Forc?d - September 26, 2016, 12:08 pm

(Sep 26, 2016 08:24 AM)warpje Wrote: [\[CITE\]](#) Learned something new nice tutorial! Will check the different RAT and crypter to see how it works with that!

Please do

It's really interesting to be able to analyze their movement a bit more detailed.

Don Genovese - September 26, 2016, 2:22 pm

Very interesting and useful, appreciate the effort gone into it.

Sc0rpian - September 27, 2016, 4:27 am

Great tutorial mate.. ! This would be very helpful for victims whose system got compromised. Also I would prefer to use 'winpatrol' tool which keeps monitor and notify user about all hidden startup programs.

Reference:

winpatrol.com/winpatrol/

LanMan - September 27, 2016, 5:35 am

Nice tutorial, it will help people, and Process Hacker is a nice little tool too.

But these tool will detect only basic malware.

[??? - September 28, 2016, 3:37 pm

Thanks for sharing, very useful information.

Ran some checks immediately after reading.

iiXenonunim - September 28, 2016, 4:32 pm

Thanks a lot for this tutorial! I highly appreciate it.

Tieko - November 5, 2016, 10:41 am

Thanks a lot for that, it's really useful.

Wherever you are, have a nice day.

Forc?d - November 5, 2016, 11:19 am

(Sep 27, 2016 05:35 AM)LanMan Wrote: [\[CITE\]](#) Nice tutorial, it will help people, and Process Hacker is a nice little tool too.

But these tool will detect only basic malware.

(Sep 28, 2016 03:37 PM)[?*****?] Wrote: [\[CITE\]](#) Thanks for sharing, very useful information.

Ran some checks immediately after reading.

(Sep 28, 2016 04:32 PM)iiXenonunim Wrote: [\[CITE\]](#) Thanks a lot for this tutorial! I highly appreciate it.

(Nov 5, 2016 10:41 AM)Tieko Wrote: [\[CITE\]](#) Thanks a lot for that, it's really useful.

Wherever you are, have a nice day.

Glad you all liked it:)

AreAno - November 5, 2016, 11:47 am

Great tutorial, thanks for sharing ;)

Condo - November 5, 2016, 1:07 pm

I will try itsoon, thx Forced :)

ChromosomeCake - November 6, 2016, 12:19 am

Thanks for this tutorial, now i feel a little safer.

LogicGeek - November 6, 2016, 12:22 am

I'm expert in this but glad to see this from you.

MaddMagoo - November 6, 2016, 4:59 am

Thanx this will save a little heartache in the future no doubt!

jademanworld - November 11, 2016, 1:55 pm

Thank you for this. My laptop fan has been running pretty loud over the past few weeks and im wondering if there's something going on in the background. Cheers

Rb.sider - November 11, 2016, 3:22 pm

Will deffo try this... seems so good

exactinaction - November 12, 2016, 1:33 am

Great tutorial , i will try it !

View - November 12, 2016, 3:11 am

Thanks for the share bro :) !!!!

choun0002 - September 9, 2017, 2:16 am

Nice Tutorial ! ? I will looking forward to your new tutorial ?

PetiteBoulette - September 9, 2017, 9:47 am

Thanks you very much for this man!! Awesome!

ProfitCoder - September 9, 2017, 10:27 am

Thanks,

Great tutorial, very interesting

Armada - September 9, 2017, 12:14 pm

7/10

Very well documented method of detection and well investigation in to suspected malicious processes. Fantastic guild for the beginners to know where to start looking at least.

Little expansion on it would be even more awesome (a few additional sysinternals apps ?) But otherwie a great starter tutorial dude, Kudos for the share.

LemonParalayses - November 9, 2017, 11:21 am

Thank you for sharing your information! I appreciate it

dragonero - November 10, 2017, 3:47 am

thank you for sharing your knowledge .

Aveling - November 10, 2017, 3:56 am

Well written tutorial, thank you for sharing this.