

Forum:[Hack Forums](#)

Thread: [process hacker shows unknown process connecting to internet](#)

lemmerule86 - June 18, 2011, 10:22 pm

hi HF

in my system hacker process showing unknown process connecting to foreign ip with UDP protocol .i have tried every thing every internet security and firewalls.but no one detecting it i am using eset smart security .

[\[IMG\]http://img62.imageshack.us/img62/3908/unknwn.jpg\[/IMG\]](#)

????

what hell no reply

no one knw that..

GI?ryallowed - June 20, 2011, 11:48 am

Well use some IP address look up to see if they end up to a company or an individual, which would mean you are RAT'ed.

lemmerule86 - June 20, 2011, 11:59 pm

(Jun 20, 2011 11:48 AM)DarkxLord Wrote: [\[CITE\]](#) Well use some IP address look up to see if they end up to a company or an individual, which would mean you are RAT'ed.

yes tried .. it shows ip from government company and also some home user might be...it use UDP protocol to connect ..with my firewall i have block all udp communication but they still can connect to ip ..i cant trace back to file as well it is not captured by any thing i tried all analysis tool but no luck ... its kind of some one is monitoring me.. help to get out of this shit...??

Conch - June 21, 2011, 12:20 am

Download Currports.

It's also a TCP/UDP analyser, except it allows you to stop processes and close unwanted ports. Make sure you close the correct ports though. or you may be in more of a mess!

Once the ports are fully closed. I recommend getting Comodo Internet Security + 1 Year free license.

Then boot into safe mode and do a full update and scan.

lemmerule86 - June 21, 2011, 2:52 am

(Jun 21, 2011 12:20 AM)Conch Wrote: [\[CITE\]](#) Download Currports.

It's also a TCP/UDP analyzer, except it allows you to stop processes and close unwanted ports. Make sure you close the correct ports though. or you may be in more of a mess!

Once the ports are fully closed. I recommend getting Comodo Internet Security + 1 Year free license.

Then boot into safe mode and do a full update and scan.

ok i am downloading this app..but abt comodo internet security . i tried it as well but no luck it can bypass firewall also ..i tried malwarebyte...when i scan ..all unknown process got disconnected to protect them self..it might be advanced worm..thank buddy i will let u know after trying that app.

buddy no luck again..have look at it

[\[IMG\]http://img33.imageshack.us/img33/9296/currport.jpg\[/IMG\]](#)

process not getting killed gives no reaction on killing process

The Ostrich - June 21, 2011, 4:31 am

(Jun 20, 2011 11:59 PM)lemmerule86 Wrote: [\[CITE\]](#) yes tried .. it shows ip from government company and also some home user might be...it use UDP protocol to connect ..with my firewall i have block all udp communication but they still can connect to ip ..i cant trace back to file as well it is not captured by any thing i tried all analysis tool but no luck ... its kind of some one is monitoring me.. help to get out of this shit...??"it shows ip from government company"

I dont know about anyone else, But to me it sounds like you did something you shouldn't of.

potti - June 21, 2011, 7:02 am

It might have "Persistence" which makes it hard to remove/kill.

I recommend just re-formatting to be safe. Back-up most files except .executables

Conch - June 21, 2011, 11:49 am

(Jun 21, 2011 02:52 AM)lemmerule86 Wrote: [\[CITE\]](#) ok i am downloading this app..but abt comodo internet security . i tried it as well but no luck it can bypass firewall also ..i tried malwarebyte...when i scan ..all unknown process got disconnected to protect them self..it might be advanced worm..thank buddy i will let u know after trying that app.

buddy no luck again..have look at it

[\[IMG\]http://img33.imageshack.us/img33/9296/currport.jpg\[/IMG\]](http://img33.imageshack.us/img33/9296/currport.jpg)

process not getting killed gives no reaction on killing process

You've isolated currports inside a Sandbox.

As far as I know, anything Isolated inside Sandbox won't function properly and doesn't make changes to the system, 'cause It's used mostly to check malware for drops and such.

Run it outside sandbox.

lemmerule86 - June 21, 2011, 11:29 pm

(Jun 21, 2011 11:49 AM)Conch Wrote: [\[CITE\]](#) You've isolated currports inside a Sandbox.

As far as I know, anything Isolated inside Sandbox won't function properly and doesn't make changes to the system, 'cause It's used mostly to check malware for drops and such.

Run it outside sandbox.did as you said but nothing happened...

bZaaaRx - June 22, 2011, 3:21 am

Go on this site [here](#) and type in the ips you think are connecting to you, and see were they are from.