

Forum:[Hack Forums](#)

Thread: [\[GUIDE\]\[Premium\] ? Protect yourself: Monitor your connections ?](#)

carecare - March 25, 2011, 7:31 pm

Protect yourself: Monitor your connections

- Difficulty (Intermediate): *****?*****?***** -

Hey and welcome to Part 1 in my new "Protection Series" first off is monitoring connections. I'm planning on writing more tutorials, that is if anyones interested. If so you're welcome to make requests!

I always try to keep my tutorials easy & direct instead of writing walls of irrelevant text.

01 Introduction

One important step in ensuring your personal security is being able to monitor your local network traffic and look for anomalies, lets face it the whole virus era is basically history, nowadays we face threats such as botnets/trojans/adware which is normally controlled by people with malicious intent who have no problems whatsoever in stealing your sensitive passwords/use your computer in various botnet attacks, that said a basic understanding of your network connections is a great step towards securing yourself from online threats. Enough talk let's get on it!

02 Table of contents

Chapter 1. Introduction to TCPView

Chapter 2. Detecting & dealing with malware using TCPView

Chapter 3. Tips

03 Tools used in this tutorial

TCPView, <http://technet.microsoft.com/en-us/sysinternals/bb897437>

CHAPTER 1

Introduction to TCPView

[img]<http://img708.imageshack.us/img708/5843/tcpcnmb.png>[/img]

1. (Process) Displays the name of the associated process
2. (PID) Displays the ID linked to the process; Process ID Number "PID"
3. (Protocol) Displays the used protocol (TCP/UDP)
4. (Local Address) Displays your address
5. (Local Port) Displays the local port
6. (Remote Address) Displays the address which the process is communicating to
7. (Remote Port) Displays the port that the process is connected to

8. (State) Displays the current STATE of the process.

SYN_SEND Indicates active open.

SYN_RECEIVED Server just received SYN from the client.

ESTABLISHED Client received server's SYN and session is established.

LISTEN Server is ready to accept connection.

9. (Sent/Received Packets) Displays in bytes the amount of data sent

What is TCPView?

In short, TCPView is a tool which monitors active processes network connection(s).

Some of you might be familiar with the built-in tool "netstat" which is excellent in terms of monitoring and detecting in/outgoing connections, however it's limited and lacks many important features, luckily there is an alternative called TCPView which is a lifesaver, it's made by the former glory [sysinternals](http://www.sysinternals.com). The beauty with this tool is that you'll be able to see and determine every processes network connection(s) without having to crosscheck the PID's in taskmanager like you have with netstat.

Some benefits of using TCPView

[?] A good replacement to netstat

[?] Easy GUI

[?] Refreshes active process states automatically

[?] Displays associated ports

[?] Great process association

[?] Generally bypasses rootkits

CHAPTER 2

Detecting & dealing with malware using TCPView

In order to demonstrate typical usage for TCPView I'll provide an image of an infected computer (see below)

[img]<http://img17.imageshack.us/img17/5188/iexpl.png>[/img]

Can you detect the malware? First off, what we want to look for here is anomalies, everything that stands out so be paranoid - malware is often characterized by:

Having unknown/odd process names

Having STATE established on weird ports

Unknown endpoints

Non logic processes (ie. seeing an closed trusted application trying to communicate outgoing, ie Internet Explorer)

Connection tampering, most malware (Trojans especially) will repetively try to connect back to the attacker - resulting in an odd network behaviour. ([see video](#))

Found it? If you haven't don't worry, it's not always easy since hackers (crackers?) work hard in masking their malware, in any case the answer is: Spoiler ([Click to View](#))iexplore.exe

Why? you might ask. First of:

1. No valid file signature/version

[img]http://img826.imageshack.us/img826/9503/ieieieieieie3423442.png[/img]

Dont be tricked by the icon, malware often mimics trusted applications! In this image you'll see that the file "iexplore.exe" has no file signature/version (In this case it should be by Microsoft) therefore it's a non-valid Microsoft application and most likely a spoof.

Quote:Do notice that some malware injects themselves to processes, if youre unsure about a file always upload & scan it on ie. [VirusTotal](#)

2. Odd file path

The file "iexplore.exe" shouldn't reside in "C:\Windows\system32" since it isn't a system file.

3. Suspicious port

Internet Explorer is a web browser, seeing it interact with ports other than (HTTP/HTTPS/80/8080) should make you suspicious.

4. IE is not visible in explorer

If you cannot see the affected program it's most likely a decoy/fake. Since every malware operates hidden.

CHAPTER 3

Tips

1. Check for connection tampering

Most malware that is controlled (RATs/Trojans/Bots etc) will always try connecting back to the attacker in intervals, I like to call this behaviour connection tampering and it's easily noticed.

If we try and terminate the connection it will most likely respawn, if it does we can safely confirm that it's a malware; ([see Connection tampering video](#))

I provied an example with a trojan in action trying to connect to it's master (process named "svhost.exe") notice the behaviour.

Quote:If the attacker already has an connection to you, it wont display this behaviour and it will have an "ESTABLISHED" state. To prevent this, try taking out the internet cable to ensure no outside connections is possible.

2. Always virus scan suspicious files

To be on the safe side always scan the suspicious file for infections, by right clicking the suspicious process we can find out what file it is associated to, if the file is a malware it has most likely already

bypassed your current antivirus so try uploading it to ie. [VirusTotal](#) / [novirusthanks](#) or any other online malware scanner.

3. Check the associated process file-signature

X Unsigned & Unverified process (svhost.exe)

[IMG]<http://img535.imageshack.us/img535/8316/fasfaas.png>[/IMG]

? Signed & Verified process (svchost.exe)

[IMG]<http://img27.imageshack.us/img27/3302/dasdasdasdsa.png>[/IMG]

Most malware claims that they are components to a trusted program (ieupdater.exe, svhost.exe, winlogon.exe, winfix.exe) In this example, svhost.exe is the malware. If a process claims to be something its not always check the files signature, if it isn't signed, it's most likely a malware.

4. Google the associated process name & port

Try a google search on the suspicious process & port number to verify if it's a legit process or not, and also to check if the port is valid.

4. Use common sense

That's right, the best defense is and will always be: to use common sense.

Let's say you find a process named "fsdgs.exe" in the active process list, it's not very likely that it's a legit child process to Windows :) don't trust any process you don't know about.

5. On suspicion: always turn off your internet

If youre suspicious and feel like something ain't right (Internet is going slow etc) simply turn off your internet to avoid further problems. As long as your connected to the internet the attacker can operate freely in your computer & cause even more damage.

~

Gebove - March 25, 2011, 8:01 pm

Looks like you've spent a lot of time on this tutorial; it's to my liking.

I was previously searching for an alternative to my network analyzer, and I think I may have found it.

As for the tutorial part of this, the determination of malware is very thorough here, great work!

Dark Molecule - March 25, 2011, 8:20 pm

really nice tutorial i always wanted to know how to do this in detail and this pretty much got me started :)

rated 5*

Dridle - March 25, 2011, 8:47 pm

Very good tutorial. I like the educational sound in it: "Can you detect the malware?" ?

You also provide many background information and the pics & video support the understanding

process very well ?

Awesome, keep up the good work! ?

carecare - March 26, 2011, 12:06 pm

Thanks for the comments :D

1luv - March 26, 2011, 1:33 pm

Great tutorial, this should come in handy!

asker - March 26, 2011, 8:27 pm

Great tutorial really...thanks for sharing it with us buddy!

Vivacious - March 26, 2011, 9:09 pm

Very detailed, I love it. Great way to detect malware/rats. Thank you so much.

To everyone else, keep this thread alive. This is very helpful and noobs need it.

ethico - March 26, 2011, 9:17 pm

nice one thanks. Keen to read your next article.

Grunt? - March 26, 2011, 10:56 pm

Thread layout enforced me to praise your work; content is good is too.

Keep it up!

-mothered- - March 27, 2011, 12:18 am

Nicely documented and Illustrated, that's quite easy to follow and comprehend.

It's quite detailed, so I'm delving Into It now.

Thanks.

Hopsin - March 27, 2011, 4:02 am

Wow mate,i am impressed. I boomed this awesome thread and i shall start testing & using this guide for safety. Many thanks mate,i really appreciate it!

im abcd - March 27, 2011, 4:21 am

seems to be useful ..thanks

John* - March 27, 2011, 4:28 am

Wow, really awesome thread. Also it's clearly explained.

Thank you, John*.

MaXoNe - March 27, 2011, 6:03 am

Nice tutorial....I used Sysinternals Suite for network monitoring and it does great work for me..

PASIØN - March 27, 2011, 6:04 am

Great guide, be sure to keep posting more handy information like this!

Regards,
PASIØN

52643 - March 27, 2011, 6:12 am

Awesome thread. Downloaded TCPView.

FOOTLONG - March 27, 2011, 2:02 pm

Nice tutorial. I'm going to try this out

Metamorphic - March 28, 2011, 7:52 am

Great tutorial something i can use, a HQ post which are rare XD
il rate this thread soon!

carecare - March 31, 2011, 2:35 pm

Thanks! I will be posting 2 HQ guides a week :)

Sr4d - April 1, 2011, 12:48 am

Very, very, very good work on this! Was an enjoyable read, a lot of good info in there!

Ty.

carecare - April 2, 2011, 12:56 pm

Thanks, glad you liked it! Next up is process analyzing :)

Syndicate - April 3, 2011, 3:00 pm

thanks for this, i have been having suspicions about a trojan hiding somewhere for awhile. I'll test this later.

Developer - April 4, 2011, 9:08 pm

I thought I had posted on this thread before.

Very good thread my friend, your work never fails to amaze me.

Kirk Gandril - April 5, 2011, 2:27 am

Nice tutorial. Very informative and easy to follow.

carecare - April 6, 2011, 11:41 am

(Apr 4, 2011 09:08 PM)TheUnknown01 Wrote: [\[CITE\]](#) I thought I had posted on this thread before.

Very good thread my friend, your work never fails to amaze me.

Thanks! And yeah the thread were first in the Hacking section, then it got moved to the Computer Protection and Security Alerts. :)

MouseDesign - April 6, 2011, 12:13 pm

Good job, I'm testing this tool for sure.

djmayur - April 7, 2011, 5:16 am

very nice tutorial....i enjoyed it..

amg64 - April 8, 2011, 11:20 pm

nice tut man, i just know netstat 2 monitor my (onn3tions..

j.diesel - April 10, 2011, 12:43 am

best tutorial i ever see!!

big vouch for you man!

Gooples - April 10, 2011, 2:03 am

Thank you, downloaded it. Will be good to monitor my processes.

kami117 - April 10, 2011, 10:46 am

Good Job Bro Tnx For This awesome Tut<<

carecare - April 13, 2011, 1:23 am

Thanks for the comments, If this reaches 6-7 pages by this week I'll promise to post part 2 next week. It's been somewhat delayed due to a hectic shedule! I'm sry.

condom - April 16, 2011, 2:43 pm

thanks bro for the tip. i got hirens boot cd v. 12 and this program is included in the cd. it works great for network analyzing.

Basics. - April 23, 2011, 7:29 am

This is an awesome guide.. Thanks for creating it!

carecare - April 24, 2011, 5:20 am

Thanks :) I know part 2-3 has been quite delayed, they will be up soon..

'HK. - April 24, 2011, 1:43 pm

Nice tutorial, I might test it out tomorrow ?

alaazizo - April 25, 2011, 11:53 am

eally nice tutorial i always wanted to know how to do this in detail and this pretty much got me started :)

hemescool - April 28, 2011, 12:48 am

Great tutorial bro Thanks for sharing

carecare - April 30, 2011, 5:44 am

Great, please report if any methods have worked :)

DaL0rd - April 30, 2011, 9:49 pm

I like this tutorial. This should help alot of people.

blem - May 2, 2011, 7:19 am

Thanks for this, will be beneficial to a lot of people.

AC130 - May 3, 2011, 8:28 pm

Doesnt look easy but promising :)

shyadonis16 - May 17, 2011, 5:29 am

nyc work....great information ?

ComX - May 17, 2011, 11:04 am

Thanks for The Tutorial mate :)

Minimal - May 17, 2011, 2:00 pm

This is actually a very good guide. Very good layout and very well written, its done that well you could even move the difficulty down to easy. Foolproof.

andie12serador - May 17, 2011, 6:02 pm

Nice. You really have a good knowledge on techno stuffs and how does it works

????? - May 20, 2011, 3:00 am

This is a very useful guide to detect if there is FUD malware in your pc

Quantumdalek - May 20, 2011, 4:14 am

Hello and thanks for this tutorial it is a HQ post indeed, bookmarked and 5 stars for you sir.

Just wanted to add a wise person told me once in another similar post where the netstat command was discussed for this same purpose, that it always comes handy to know how to do those things using only Command Prompt, even if it is slower and more complex, it gives the user a much needed level of skill to solve software problems, and honestly I sometimes believe DOS commands are almost as powerful as Linux Terminal, a very useful tool not to be forgotten or underestimated.

That said I think I know at least 2 other programs that do a similar task to "TCPView", and I say similar because since Im a noob in this field Im not completely sure but at first sight they look twin applications, one is [NirSoft CurrPorts](#) and the other (my favorite and the one I see more advanced) is [Process Hacker](#), both freeware and safe utilities as long as I can tell.

Again thanks for this HQ tutorial please keep them coming.

Dozy Van - May 21, 2011, 4:22 am

wow... epic guide man ty.

and keep up the good work

Lightangel - May 22, 2011, 5:29 am

Rated 6/10.

Nice graphics and well explained.

It's a really helpful tutorial.

Gonna give it a try.

PrO1337HaCKeR - May 22, 2011, 10:12 am

this is a very nice tut, it helped me find a weird program that aparetly slowed down my internet becuasae it was downloading something or i guess it was torrenting....

carecare - May 25, 2011, 5:50 am

(May 20, 2011 04:14 AM)Dalekboot Wrote: [\[CITE\]](#) Hello and thanks for this tutorial it is a HQ post indeed, bookmarked and 5 stars for you sir.

Just wanted to add a wise person told me once in another similar post where the netstat command was discussed for this same purpose, that it always comes handy to know how to do those things using only Command Prompt, even if it is slower and more complex, it gives the user a much needed level of skill to solve software problems, and honestly I sometimes believe DOS commands are almost as powerful as Linux Terminal, a very useful tool not to be forgotten or underestimated.

That said I think I know at least 2 other programs that do a similar task to "TCPView", and I say similar because since Im a noob in this field Im not completely sure but at first sight they look twin applications, one is [NirSoft CurrPorts](#) and the other (my favorite and the one I see more advanced) is [Process Hacker](#), both freeware and safe utilities as long as I can tell.

Again thanks for this HQ tutorial please keep them coming.

Hey thanks, yeah it's always good to be familiar with the basics aswell, such as performing a netstat lookup etc.

tidus091 - May 28, 2011, 2:42 pm

Great tutorial...thanks for sharing it ?

carecare - October 9, 2011, 3:38 pm

Thanks for the feedback everyone :D

Bass.exe - October 10, 2011, 3:16 pm

I was very impressed by this tutorial. I will use this tool often thanks to you.

carecare - October 10, 2011, 3:47 pm

Thanks, I think this guide should be stickied in this forum category - it basically covers 80% basic network security and by my definition the guide is easy to understand.

Who do I ask for this?

?Shrewd - October 12, 2011, 2:42 pm

that was a really good and well organized tutorial. really helped me out and I learned a lot of new stuff! :) Thanks for great tut mate

throughhymn - October 15, 2011, 10:11 am

Thank you for this wonderful guide! but when we find things that dont bleong, how do we get rid of them? simply running virus scans, etc?

carecare - October 16, 2011, 4:19 am

(Oct 15, 2011 10:11 AM)throughhymn Wrote: [\[CITE\]](#) Thank you for this wonderful guide! but when we find things that dont bleong, how do we get rid of them? simply running virus scans, etc?

Hey yeah that's the best way of doing it, but if you may have to remove them manually since they obviously bypassed your antivirus software.

DsntExist - June 27, 2012, 11:22 am

Thanks bro, really a good way to stop RAT connections out there. Never thought of using a method like this before.

jeffmacky - January 3, 2013, 7:44 pm

Thanks man! Was searching for this on google but found the real info here.

johnnyj - January 3, 2013, 8:45 pm

Thankyou. Going through some threads here and now finding myself checking if all my connections are legit.

r3v34 - January 4, 2013, 12:53 pm

Appreciated your work. Good understandable. Every day something new to learn ?

HexUness - January 4, 2013, 1:42 pm

Thank you for this great tutorial :)

pure_d4m - January 5, 2013, 1:24 pm

Very detailed thanks.Hope you will make more threads like this