

Forum:[Hack Forums](#)

Thread: [\[TuT\] \[HQ\] How to Test Your Malware For Connection \[TuT\] \[With Pictures\]](#)

NoodleBot™ - January 19, 2014, 2:21 pm

Hey there. I'm seeing a lot of frustration, with new members as well as some of our experienced users having trouble setting up these RAT's[b].

If you are going to be involving yourself with any Keylogger, RAT, stresser, bruteforce or cracker tool, definitely consider some form of protection to cover yourself.

Check out my latest program Absolution, aimed at providing a safer environment and settings that are easy to configure.

My goal here today is to bring to you a very simply walkthrough that will show you how to test your keylogger, your RAT, your botnet, your Java drive by, and even your exploit kits, without requiring to use another system, test installing on a friend or bot, and should be well known to everyone that wants to test their own files, and even other peoples files!

- How to Test Your Malware For Connection -

By

NoodleBot™

Steps before proceeding

Ensure you have the proper software to work with here. Today, we'll be using Sandboxie, by Ronen Tzur.

Sandboxie website - <http://sandboxie.com/>

Sandboxie direct download: <http://www.sandboxie.com/SandboxieInstall.exe>

Sandboxie version 4.06 ... Released on 16 October 2013

Notes:

If you have followed any of my previous walkthroughs, the malware you have built properly will already contain your localhost and No-Ip/VPN information, so you will be able to test & spread the same server with no issues.

Additional notes will be at the bottom of the thread.

Before proceeding - PLEASE READ

What is Sandboxie?

Sandboxie is a sandbox-based isolation program developed by Ronen Tzur, for 32- and 64-bit Windows NT-based operating systems. It creates a sandbox-like isolated operating environment in which applications can be run or installed without permanently modifying the local or mapped drive. An isolated virtual environment allows controlled testing of untrusted programs and web surfing. -

<https://en.wikipedia.org/wiki/Sandboxie>

Step 1:

After downloading and installing Sandboxie, you want to begin by deleting the Sandboxed Browser shortcut off of your browser, and then hit Start and type Sandboxie Control

Move this file to your desktop instead - it is the control panel and will serve as your task manager.

Step 2:

Open up Sandboxie Control. At this time there is no need to change any of the settings, unless you have a specific program you want to shove into sandboxie and grant harddrive access or UAC access but you do not need to worry about that at this time.

To begin, we should test sandboxie control and see how it functions, and how this can be beneficial to us.

So I have set up a simple simulation, to help imagine how this can help defend yourself from other attackers online in the wild.

In this first screenshot, you can see the example program I have tested with to demonstrate how files can be binded to one another.

In this second image, you may now see how I have binded my RAT to it and how it would appear to run on a windows system.

Successful connection from self testing.

So now that you see how it works, all you have to do (providing you followed my walkthroughs) is drag and drop your .exe file into the Sandboxie Control and watch it run.

If the file has run and you see no connection, this may mean your ports are closed or there is an error with the file.

Step 3: To be taken if testing a Java Drive by or Exploit Kit

So now you've figured out how to run your .exe's and .jar's and whatnot through sandboxie. Now let's take it up one notch further and try running your Java Drive by or Exploit Kit inside a Sandboxed web browser!

Right click your sandbox and select, Run Sandboxed > Run Web Browse

After running the traditional Java Applet as seen here, you can also begin to see your file download and be executed!

Before running applet:

After running applet:

And there you go!

Testing your own malware has never been easier.

Additional Notes:

- You should always Delete the contents of your Sandbox's. Always remember to terminate all programs and then delete the contents safely.

- I'm a terrible photo uploader/editor

- You may find the rest of my walkthroughs below,

All my walkthroughs can be found here!

<https://hackforums.net/showthread.php?tid=3012187>

Darkcomet

<https://hackforums.net/showthread.php?tid=3012160>

Cybergate

<https://hackforums.net/showthread.php?tid=3012223>

Blackshades

<https://hackforums.net/showthread.php?tid=4002020>

nJrat V0.7D

<https://hackforums.net/showthread.php?tid=3020657>

Portforwarding

<https://hackforums.net/showthread.php?tid=3970786>

How to Securely and Properly use your VPN Server

<https://hackforums.net/showthread.php?tid=3679336>

Tutorial | How to Take Ownership of a Folder and Files Inside

<https://hackforums.net/showthread.php?tid=4035882>

Tutorial | Clear Event Viewer (All System/Network Logs)

<https://hackforums.net/showthread.php?tid=3679339>

Tutorial | How to Restore Original System Ownership a Folder and Files Inside

<https://hackforums.net/showthread.php?tid=3661066>

Tutorial | How to Dual Boot Kali Linux + Windows 7

<https://hackforums.net/showthread.php?tid=3832986>

How to Spoof your MAC Address

<https://hackforums.net/showthread.php?tid=3751307>

[White]Black Hat] Tutorial | Instantly Restore Access to Task Manager

<https://hackforums.net/showthread.php?tid=3751305>

Tutorial | How to do a Deep Scan of your Computer - BY HAND -

<https://hackforums.net/showthread.php?tid=3892799>

[TuT] How to INSTANTLY Customize your Mac Address [TuT]

<https://hackforums.net/showthread.php?tid=3892781>

[TuT] How to Secure a Hacked / Rented RDP [TuT]

I hope that I can help you and if you still require any assistance feel free to shoot me a PM.

Enjoy!

Razza™ - January 19, 2014, 2:23 pm

Noodle's jimmies got rustled.

Nice guide man.

Disfigured - January 19, 2014, 4:41 pm

Nice to read this, i thik is a really good idea share this infomation. Congratulation for u great job.

HackScope - January 19, 2014, 5:11 pm

Nice guide that was a smart idea of sharing this

Shike - April 3, 2014, 3:00 pm

Thanks for this! Appreciate it a ton :) worked well for testing

iDuL - April 3, 2014, 3:18 pm

Thanks for such a noob-friendly tutorial OP!

mrtwothree - April 7, 2014, 9:04 pm

Just wanted to say that you are my hero.

Seriously thank you for posting these, they helped me out immensely. Stupidly my network got infected with some persistant trojan/rootkit that didnt show up in any AV. These guides helped me go through and clean things up as best as I could. Im still cleaning up one of the pcs because literally 3 of them got infected but you info helped me get things right.

I appreciate bossman.

If you need any help, dont hesitate to ask, I hope I can repay the favor in some way.

NoodleBot™ - April 7, 2014, 11:35 pm

(Apr 7, 2014 09:04 PM)mrtwothree Wrote: [\[CITE\]](#) Just wanted to say that you are my hero.

Seriously thank you for posting these, they helped me out immensely. Stupidly my network got infected with some persistant trojan/rootkit that didnt show up in any AV. These guides helped me go through and clean things up as best as I could. Im still cleaning up one of the pcs because literally 3 of them got infected but you info helped me get things right.

I appreciate bossman.

If you need any help, dont hesitate to ask, I hope I can repay the favor in some way.

I'm glad this could help someone out! I see lots of threads being started when all it requires is a little reading.

Mr.ProVanzla - April 16, 2014, 2:04 pm

Good tut thanks for this and background fucking perfect

NoodleBot™ - April 16, 2014, 2:24 pm

The background is here, and thanks!

Spoiler [\(Click to View\)](#)

<http://minus.com/i/bhBQHGC6yyIEt>

Cyberspirit - April 23, 2014, 5:03 am

Woaw great list of walkthroughs... i will read them all ... ty mate !!!

MrCortex - April 23, 2014, 10:27 am

This is one rock solid tutorial man thanks for the information ... you give me some new ideas to start with because normal I use vmware to make a virtual machine to test on it but this is a lot easier and it use a lot less resources

NoodleBot™ - April 23, 2014, 1:37 pm

(Apr 23, 2014 10:27 AM)MrCortex Wrote: [\[CITE\]](#) This is one rock solid tutorial man thanks for the

information ... you give me some new ideas to start with because normal I use vmware to make a virtual machine to test on it but this is a lot easier and it use a lot less resources

If you really wanted to take the precautions (and avoid reinstalling vm if shit hits the fan) you could run sandbox inside your virtual machine.

MrCortex - April 25, 2014, 10:19 am

(Apr 23, 2014 01:37 PM)NoodleBot™ Wrote: [\[CITE\]](#) If you really wanted to take the precautions (and avoid reinstalling vm if shit hits the fan) you could run sandbox inside your virtual machine.

Uhhh this is indeed a good idea ... thnx man ?

dumosz - April 11, 2015, 6:56 am

thanks for the help. Glad to see there are people helping noobs instead of ignoring them. Everybody's got to learn, right. Thank you

Linkin™ - April 11, 2015, 6:58 am

Just a note: Not all people have NAT Loopback therefore their DNS will not work on their own system. To overcome this issue create a seperate stub with the same port but your IPV4 Address (e.g. 192.168.86.1) or your localhost IP address (127.0.0.1), I think you should add this into the guide.

Linkin

NoodleBot™ - April 11, 2015, 4:02 pm

(Apr 11, 2015 06:58 AM)Linkin Park Wrote: [\[CITE\]](#) Just a note: Not all people have NAT Loopback therefore their DNS will not work on their own system. To overcome this issue create a seperate stub with the same port but your IPV4 Address (e.g. 192.168.86.1) or your localhost IP address (127.0.0.1), I think you should add this into the guide.

Linkin

As in all the other threads that may have brought you here; (not sure how you got to this one) that is covered in BUILDING process rather than testing, to avoid this confusion later on.

<https://hackforums.net/showthread.php?tid=3012187>

Darkcomet

<https://hackforums.net/showthread.php?tid=3012160>

Cybergate

<https://hackforums.net/showthread.php?tid=3012223>

Blackshades

<https://hackforums.net/showthread.php?tid=4002020>

nJrat V0.7D

<https://hackforums.net/showthread.php?tid=3020657>

Portforwarding

Linkin™ - April 12, 2015, 1:49 am

(Apr 11, 2015 04:02 PM)NoodleBot™ Wrote: [\[CITE\]](#) As in all the other threads that may have brought you here; (not sure how you got to this one) that is covered in BUILDING process rather than testing, to avoid this confusion later on.

<https://hackforums.net/showthread.php?tid=3012187>

Darkcomet

<https://hackforums.net/showthread.php?tid=3012160>

Cybergate

<https://hackforums.net/showthread.php?tid=3012223>

Blackshades

<https://hackforums.net/showthread.php?tid=4002020>

nJrat V0.7D

<https://hackforums.net/showthread.php?tid=3020657>

Portforwarding

I understand but some people may use their DNS as majority of my customers on RAT setups didn't know this. So if they used their DNS on this tutorial they'd assume it's not working, so this is just a reminder to them.

NoodleBot™ - April 12, 2015, 12:59 pm

(Apr 12, 2015 01:49 AM)Linkin Park Wrote: [\[CITE\]](#) I understand but some people may use their DNS as majority of my customers on RAT setups didn't know this. So if they used their DNS on this tutorial they'd assume it's not working, so this is just a reminder to them.

I guess, but that's why I made the walkthroughs the way I did in the end.

classscore - April 14, 2015, 3:53 am

There's several ways you can do this. They make hnets for this.

HQ Post though.

GOD OF SARADOMIN - November 29, 2015, 12:42 pm

Nice Tutorial Bro , i just saw that thanks for your work !

minato44222255 - June 24, 2016, 4:03 am

Hey can i know which rat you used?

NoodleBot™ - June 24, 2016, 12:00 pm

(Jun 24, 2016 04:03 AM)minato44222255 Wrote: [\[CITE\]](#) Hey can i know which rat you used?

The process will be the same for testing your stub. It doesn't matter what I used - a stub is a stub but you can see how with my other walkthroughs.

iNeed Sleep - June 24, 2016, 12:14 pm

Great tutorial, thanks for sharing this information. A lot of users do struggle with testing their malware and this will def alleviate a lot of usual "halp pls" questions.

Patzan - June 24, 2016, 7:23 pm

working so good! now i can test easyyyy

retherenn - June 30, 2016, 10:41 am

I can't thank you enough for this tutorial. But I will try my best. Thank you.

MiSHo - December 22, 2020, 6:12 pm

thanks bro , good job i always use sandboxe