

# Forum:[Hack Forums](#)

Thread: [VirusCheckMate Proposed Testing for Distribution](#)

**CyberStrike** - February 13, 2018, 2:09 pm

I have seen many threads regarding whether or not VirusCheckMate is distributing or not. Before deploying out in the field I would like to get the opinion of the members on the proposed testing methodology.

- 1) Using a base file as a template I will make it rather fud it will or should look rather new, a few detections are infact OKAY we just have to note them.
  - a) Upload the full file to VirusCheckMate and note any detections as well as identified signatures
- 2) Divide each section of the file for example .text ..etc and place into new executables which we can upload after a set amount of time from initial upload to VirusCheckMate ( enough time for the AV companies to have time to get their matching if there is distribution)
- 3) Compare results between VirusCheckMate (having the full file) and NoDistribute/VirusTotal (only sections of the file) noting differences in the number of detections as well as identified signatures.

The reason we upload several small files is so then no one AV maker should have a full payload unless VirusCheckMate does distribute.

Also using common methods such as hyperion or PE Scrambler or common crypters will not be used on any of the files I would hate to have detections due to usage of a crypter. Also if there is distribution well sending out a crypted file isn't the best move. So all obfuscation will be done manually.

Reason for waiting : To allow AV makers to possibly get a signature as well as distribute the file amongst themselves. Also without a set time frame no one will stop all business till such testing is over.

Tools to be used:

-----  
readpe  
objdump  
objcopy  
ghex  
file  
pedump  
pefile

Ensuring file integrity is important and I propose that the file will let us know of any issues with our headers so each file is properly identified as an executable. Second the sections must be the correct size/offset/flags...etc. Using objcopy and objdump we should be able to verify all of this information also we must make sure that each section's hash values match up, using pefile.

I am looking for possible flaws in this testing methodology as to have accurate information and results, which will be published here in full after completion.

**P.E.Investigations** - February 13, 2018, 3:03 pm

Hm. It seems to become a lot of work. How do you divide each section? About equal length?

**CyberStrike** - February 13, 2018, 4:06 pm

For each section I'll be using 'objcopy -j .section file out\_file' I already have double checked and before hand I will get the hash value of each section, I want to make sure that I am not changing anything between the original submitted file to VirusCheckMate and the files that will be broken up. I will be using sha256 for this simple before submission if the hashes for the sections do not match it will not be submitted and considered invalid.

It's not hard maybe tedious but I use the same techniques for doing AV evasion finding signatures that AV's hit on and if possible changing it as per "Taking Back NetCat" and same idea as AVSignSeek, which I discussed in another thread.

**Purple Kief** - February 13, 2018, 4:48 pm

If there is anything I can do for you (I doubt it) please do let me know.

**CyberStrike** - February 13, 2018, 5:01 pm

I appreciate it, I will do a full write up btw so you guys can pretty much re-create the steps as well, there is no "hidden/private/secret" methods which I hold back.

**Sheeple** - February 13, 2018, 5:03 pm

Why VirusCheckMate someone prove that Nodistribute does or doesn't distribute.

**CyberStrike** - February 13, 2018, 5:26 pm

(Feb 13, 2018 06:03 PM)Sheeple Wrote: [\[CITE\]](#) Why VirusCheckMate someone prove that Nodistribute does or doesn't distribute.

Tell ya what I can do that as a test then move onto VirusCheckMate. It's a good idea to see if the methodology will work. I will post all the results here, I just ask that everyone please leave the first do not rescan it because I will scan it on VT but only the sections the files.

**Sheeple** - February 13, 2018, 5:29 pm

(Feb 13, 2018 06:26 PM)sirru5h Wrote: [\[CITE\]](#) Tell ya what I can do that as a test then move onto VirusCheckMate. It's a good idea to see if the methodology will work. I will post all the results here, I just ask that everyone please leave the first do not rescan it because I will scan it on VT but only the sections the files.

Thank God. Finally that fucking rant can be dealt with. Thanks :D Just NoDistribute is like the #1 Speculative site on HF for distribution that's why I brought it up. Shit I remember like August 2017 I could swear on the daily there were multiple threads

"Nodistribute distributes"

"I mass distribute my file, but only scan on NoDis so it distributes"

"It's a eset honeypot - Nodistribute"

"I have no idea what I'm talking about, but NoDistribute distributes"

**Viotto01** - February 13, 2018, 6:16 pm

Some AntiVirus software such as ESET will send samples even if you uncheck their options.

To be totally safe, VirusCheckMate should run the sample in a snapshot without internet connection, then delete snapshot at end of analysis.

**CyberStrike** - February 13, 2018, 8:21 pm

I have to come clean really didn't think about NoDistribute originally, but I had in fact done a similar test not quite as involved as what I am proposing here, but let me just share the results from that

experiment.. I used Netbus1.6 (of course nothing amazing just dealt with as many AV signatures as I could takes a long while btw.. like I need about 1 day to prep up for each of these tests.. ) and maybe if I used something "newer" as a base file it maybe a bit easier.

I prepped the file using msfvenom just for obfuscation, one should note that shikata\_ga\_nai some AV's will hit on that so we use the jmp\_call\_additive to further help with a few of these detections. Now we are ready to bring PATCHYedit.EXE to our hex editor, for saftey we always make backups. For this work I make a copy in another directory that is now our working directory. Now we are going to split up this file into various sections and bring it to our Windows 7 VM runinng Kaspersky/Mcafee/Norton. This technique is used in "Taking Back NetCat".

```
msfvenom -a x86 --platform windows -x 'PATCHYUPX.exe' -k -b '\x00\x41\x08' -e shikata_ga_nai -i 2 > msfvenom -a x86 --platform windows -e x86/jmp_call_additive -i 3 -f exe > PATCHYedit.EXE
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/jmp_call_additive
x86/jmp_call_additive succeeded with size 29 (iteration=0)
x86/jmp_call_additive succeeded with size 61 (iteration=1)
x86/jmp_call_additive succeeded with size 93 (iteration=2)
x86/jmp_call_additive chosen with final size 93
Payload size: 93 bytes
Final size of exe file: 50688 bytes
```

Just for further obfuscation I pumped up the file using 'truncate -s +21kb Patchyedit.EXE (OF course make a backup).

```
md5sum
09e4b8f31e9e6fa1d1b8df2c7109bb06 PATCHYedit1.EXE
```

```
sha256sum
35e8ee6a890657899153e18b6d7f6cdf9c047f42320060f2b021df8041ca466e PATCHYedit1.EXE
```

Size: 73802 Feb 7 16:55 PATCHYedit1.EXE

\*\* I ask that no one please scan or re-scan the file to let the community draw their own conclusions\*\*\*\*\*

Either way NoDistribute at first had 2/37 .. Detections on were by ClamAV & MS Security Essentials

Spoiler ([Click to View](#))

I waited about 6 hrs later then uploaded the same file to VT 5/62 .. the ClamAV and MS Security Essentials detected as expected .. but now I had Kaspersky detecting as well, which was the same between both of these two different scanners.

<https://www.virustotal.com/#/file/35e8ee6a890657899153e18b6d7f6cdf9c047f42320060f2b021df8041ca466e/detection>

\*\* I ask that no one please scan or re-scan the file to let the community draw their own conclusions\*\*\*\*\*

Edit: These are not widely distributed files and I do these tests to further understand how AV works so unless there is an underground community of NetBus users this isn't a normal to see RAT, while yes the msfvenom encoders may hurt the detection rates .. let's face it 2/37 and 5/37 isn't too awesome and 6 hrs earlier I got around Kaspersky, unless the updates are different between them. I am retiring NetBus btw I will be trying to find BO2K or something relatively old, since they have not been seen for a while.

To confirm the previous results I went ahead and grabbed Back Orifice Remote Administration System v1.20 7-30 (Circa 1998) .. it has gone up to NoDistribute currently it has 1 detection .. from Norton I will give it about 12 hours then upload the same file to VT and see what new AV's if any catch the file.

Edit to the Edit: Uploaded test file to VT after ~12 HRS 1 extra detection

\*\* I ask that no one please scan or re-scan the file to let the community draw their own conclusions\*\*\*\*\*

NoDistribute 1/38

Spoiler ([Click to View](https://NoDistribute.com/result/image/joPZ8YxiFyDVmwHc.png))<https://NoDistribute.com/result/image/joPZ8YxiFyDVmwHc.png>

VT 2/62

<https://www.virustotal.com/#/file/a2be320f014910e8d4921ec66a3833f6cd578ad282da89ba574eda02f0152e01/detection>

\*\* I ask that no one please scan or re-scan the file to let the community draw their own conclusions\*\*\*\*\*

**CyberStrike** - February 27, 2018, 8:18 pm

Quite sure they distribute in the first test kaspersky hit on it 6 hrs later on VT .. my second test I found I had made a small mistake so unless it was analysed by a person they wouldn't see what it was trying to do. Next I want to do VirusCheckMate.

Edit: These files were all one off I handled for the most part as many AV signatures as I could so they are not spread all over or anything of the sort.

**DutchGreen** - February 28, 2018, 6:45 am

Nice project. PM me if you need any help.

Would love to hear the results on VirusCheckMate, since I'm fairly sure NoDistribute distributes ?

Good luck ?

**cryptocom** - March 1, 2018, 11:31 am

"I have no idea what I'm talking about, but NoDistribute distributes"

**Sheeple** - March 1, 2018, 11:42 am

(Feb 28, 2018 07:45 AM)DutchGreen Wrote: [CITE](#) Nice project. PM me if you need any help.

Would love to hear the results on VirusCheckMate, since I'm fairly sure NoDistribute distributes ?

Good luck ?

?????

<http://prntscr.com/iljl61>

<http://prntscr.com/iljl61>

<http://prntscr.com/iljl61>

?????

**CyberStrike** - March 1, 2018, 6:32 pm

(Mar 1, 2018 12:31 PM)cryptocom Wrote: [\[CITE\]](#) "I have no idea what I'm talking about, but NoDistribute distributes"

DutchApple also had one of his files detected after using NoDistribute. Also if you got any better testing methodology please suggest, because we don't want bad results or bad methodology so others can replicate and verify the results.