

Forum:[Hack Forums](#)

Thread: [\[MUST SEE\] The RAT's Crew \[Tips 'n Tricks \] || Week #2 \[UPDATED\]](#)

Kill?Muvz - June 4, 2011, 8:30 am

[img]http://bit.ly [WARNING: potentially infected]/ivKhuv[/img]

IF YOU ARE READING THIS PLEASE READ MY SIGNATURE!

Hello fellow HF members, I'm here to present with a brand new, noob-friendly weekly guide. I'm here demonstrating the knowledge that The RAT's Crew has, and for next weeks I will be covering multiple subjects on R.A.Ting and all that it involves. I with the help of several other members will provide extensively detailed information on every subject.

WEEK #1 - See it [HERE!](#)

For the second week I'm going to cover the intermedian of R.A.Ting which is:

Security/Protection

File undetection / encryption, what it is, what it does.Settings using .net crypters, vb6 and c++.

Sources download link.

Methods: FileSplit+HEX Editing

Introduction to Spreading.

Tips 'n Tricks.

Security / Protection

Well after reading my first edition you might be thinking it is all safe. How can anyone catch me?
There are some easy ways to do it, seriously.
Such as:Reverse engeneering (No one would waste time doing that.)

Simply click Start > Run > CMD > Type netstat -a > Look out for any strange IP you do not recognize > Trace it.

Using tools such as WireShark.

So what can I do to prevent me from getting caught?

Lets think a bit, if you stablish a connection it will appear on the netstat right?

Well what if you DON'T stablish one? Get it?

So with this we have 2 different methods, and an extra one which is sort of useless. Using PHP R.A.T.'s. Why? Well read the previous week edition and you'll see that PHP R.A.T.'s do not connect directly, therefore your IP will not be visible to netstat or any other method.

This is now a bit more "advanced" > [Blackshades R.A.T](#) [One of the best R.A.T.s out there] has a really unique feature : Asynchronous Mode! What is that all about? Well on asynchronous mode You (your client) will only re-connect every 5 mins , or any other time interval, to check if they are still online, or when you decide to send them any command. Efficient right?

VPN (Virtual Private Network). You can think of a VPN as tunnel (VPN tunneling), if I were to explain it all it would take ages. So short and to the point. It work like a proxy, but for every single connection you do. Let's say your IP is 1XX.XXX.X.XXX , while using a VPN your IP will automatically change to the VPN's. Therefore if they try to hunt you down they'll fail miserably as they will only be able to trace the VPN. This will work for every connection you make. Yet, there has to be a bad side. Most of the VPNs for sale keep loggs and do not have open ports, thus making them pretty much useless because you'll need your ports forwarded. They are not for free. Anyway, if you're trying to buy a VPN look out for the loggs part and the ports. Some exemple "RATing compatible" VPNs : [Blackshades VPN](#).

Ok, so now you've got an idea on how to not get caught.
Moving on.

File undetection / encryption

You've got everything set up right? and you want to start infecting people. You've tried to send it to a friend and his Anti-Virus popped up and deleted the file?

Well Anti-Virus companies are smarter then you thing. They update everyday with new virus / malware signatures. Meaning your virus some day, some how WILL be detected.

But how can I at least make if Fully Un-Detecteable for a period of time?

That's why there are these freaky tools that do things begginners could not have imagined. Those tools are called Crypters or Obfuscators.

So what they will do is cover up your Virus to make it FUD!

How does it work?

It's a bit complex so I'll cut it short.

A Crypter can be: Scantime : When the A-V runs a scan on your PC it will not be found, this is if your piece of malware is STILL FUD. Or when you simply check online if it is FUD using some online scanners such as My-AvScan.com or Scan4You.

Runtime : This is the most common, and loads of free crypters only are Runtime FUD. Meaning they are undetecteable while running the PC normaly without making the A-V go berserke, BUT once the user decides to do a system scan the server WILL be detected, even if it still is FUD runtime. Crypter will need a RunPE to make it Runtime, as the runPE injects the server into a

process.

Or both. If you're planning on buying a Crypter make sure it if Scan and Run time FUD .

Crypters work with this little .exe called STUB. The stub is the most essential part. What the crypter does is to "join" the stub with your piece of malware. The stub will "cover up" the malware making it non-readable while encrypted, thus making it invisible to the A-V engines. After the Crypted file is run the stub will drop the file in a directory and decrypt it with the encryption password and run it.

Here's some images to clear things out:

[img]<http://dl.dropbox.com/u/19745684/22.jpg>[/img]

[img]<http://dl.dropbox.com/u/19745684/images.jpg>[/img]

Downloaded a Crypter but there is only ONE .exe?

It is because these tools can have: External Stubs : You'll find an .exe or a .dll file on the crypters folder.

In-built Stubs : These have the stubs "inside" the crypter, therefore no need to have more then one .exe file.

Just to add to your vocabulary. There's a BIG difference between FUD and UD. UD, Un-Detectable means ONE OR MORE AntiVirus accuses your file as an infection. FUD is ONLY when NO AntiVirus accuses an infection.

Crypters also can be DEPENDENT or NON-DEPENDENT.

~The most common dependencie is .Net Framework. Using a crypter written in VB.Net or C# will make your server dependent, meaning the victim you try to infect will have to have installed in his machine a version of DotNet Framework. That can be considered a bad thing, yet any version of windows latter then Windows XP sp2 will have it installed, so considering the odds of having a dead computer that doesn't even has SP2 it will work pretty good.

Java Crypters are also dependent, the victim will have to have Java installed on his machine.

Any other language like :C++ / ASM

Delphi

VB6

Are NON-Dependent, meaning it can be ran in ANY Windows OS machine.

Now to broad your knowledge a bit more: USG. Unique Stub Generator is a "stub maker" as you might have got by the name. It creates a whole new unique stub from the one you used before, making stubs less equal, meaning that IF a stub you generated gets detected using another stub created by USG the chances are that one will be FUD.

This also can be: In-built. (Most Crypters)

External (i.e. Fly Crypter)

Here are some crypter's sources for you to study if you want to learn a bit more about how they

work!

[img]http://bit.ly [WARNING: potentially infected]/j5Emfc[/img]

Spoiler ([Click to View](#))

Click [HERE](#) for my thread FULL OF SOURCES!

(Had to use a separate thread. Words limit reached.)

For now we are done with the crypters.

Anyway...

There are tons of other ways to FUD your malware.

One of them is Hex Editing. In this edition I'll cover the simple method of Hex editing (the easier and less time consuming) which is basically: File Splitting + Basic Hex editing.

Why is Hex editing necessary here?

Well as you might have read before in this thread some signatures are tagged by some AntiVirus, thus changing them with Hex editing will make those detections go away.

(Don't go all ninja and change everything. If you do that you'll surely corrupt the .exe)

File Split + Hex Editing

Spoiler ([Click to View](#))

You'll need an Hex Editor. You can use [/koKazL\]THIS](#) free one.

Pick the server you want to edit (Recommended Uncrypted, but otherwise is good too.)

Turn off your A-V (Results may vary, it all depends on your AntiVirus, so pick a good one).

Now place your server in new folder. Rename it to test.exe. If you scan it now you'll see it is detected!

Open the File Splitter and Calc.exe [Start>RUN>Calc.exe].

Open the server you want to split in the FileSplitter and choose Custom Size. You can see my server's size is 53,495 bytes and I want to split it into 4 pieces. Go to Calc and divide 53,495 (Use your malware's size) by 4. Type the result in the Custom Size box, like in this image. Click on Split.

[img]http://bit.ly [WARNING: potentially infected]/mQpBI0[/img]

Your folder should look like this with the splitted files.

[img]http://bit.ly [WARNING: potentially infected]/k0DnMI[/img]

Scan the files, the ones which get detected will have to be split again. After finding out the one who causes the detection create a new folder named the number of the that was detected. My detected part is #3.

Browse to test.exe.3 (your file that caused detection), split it again using the same method (Calc.exe and divide the size by 4, again). Change the output folder to the one you just made on the step before. Mine will be 3.

[img]http://ploader.net/files/96d248fe3dbff6967200d966b6427cb9.png[/img]

The new folder should look like my folder 3 looks like.

[img]http://ploader.net/files/7c6d020fc5c1003ef17d09b2947985d7.png[/img]

Re-Scan. Find the part causing the detection. My detected part is test.exe.3.3. So I'll make a subfolder, name 3.

Browse to the file, on File Splitter, that got detected. Mine was test.exe.3.3. For the output directory choose the subfolder you just made, mine will be 3.

[img]http://ploader.net/files/d10ef6d6a8d1c032d150a9da725439a6.png[/img]

Scan all files again. Find the one causing the detection. Mine was test.exe.3.3.4, so follow I'll make a new folder named 4.

Browse the detected file in File Splitter. Mine, test.exe.3.3.4, and for the output folder choose the one you just made, mine is 4.

[img]http://bit.ly [WARNING: potentially infected]/jBJsF9[/img]

Re-Scan, find the one that acused detection and open it in the HEX Editor. If it is too big continue splitting and finding the detection. If not, proceed.

Ok. My detected file is test.exe.3.3.4.1 . So I'll open it now. It will look something like this.

[img]http://bit.ly [WARNING: potentially infected]/l4gnva[/img]

Now the Virus Signature is in here. All you really have to do is change a letter from capital to a lower case one. I changed "D" to a lower case "d" from the word DLLHOOKSTRUCT.

[img]http://bit.ly [WARNING: potentially infected]/k77AJ9[/img]

Save it. Scan it. CAREFULL, Do not do it too randomly, it CAN corrupt your malware.

Now re-compiling. I'll show one step, the rest is just the same.

See the file splitter icon there? Click it and it will recompile.

[img]http://bit.ly [WARNING: potentially infected]/itp37L[/img]

Copy that file and paste it in the previous folder. Replace it. Do the same you did previously. And continue copying pasting, recompiling untill you get to the first folder.

Done!

We will not cover full HEX editing. Why? There are thousands of tutorials for it. Simply use the search button.

Spreading

At this point you have to know what spreading is. If not, spreading is "sharing" your malware with multiple people, over the internet, with the intention to get them running your server. There are multiple methods. In this edition we will just show the types of spreading.

There are TWO types of spreding: Targeted : This means to a specific group, type of people, or to a single person.

Un-targeted : This is also the "RANDOM" spreading. You do not direct it towards any group. You simple want people to run it. For this you can use Youtube Videos, Torrent, Post in Forums, and many other thing.

On the next edition we will teach you some effective methods.

TIPS: NEVER, but NEVER, scan your files in VirusTotal.com . They will distribute your sample to AV companies making your stub detected faster. You can use online scanner such as novirusthanks.org (ticking "do not distribute sample"), my-avscan.com, OnlineCrypter.com, Scan33.com, and some others.

For the spreading part, here are some things that will help: Untargeted Bind it] with a fake program. A keygen is the best way. Pretend it is a keygen for a very good program. For me Adobe collections CS5 worked pretty good. Windows come with a binder, iexpress.exe . There are plenty of tutorials on how to use it.

Use your imagination, innovate.

Targeted This is the only type of spreading I do. Why? More profit for me. I usually target my teacher and it works. How? Well simply say you are having difficulties resolving a worksheet you found on the internet (And never say it is you, always give someone else's name.).

[HERE](#)'s me inside my teachers PC. BUT if you're doing this, PLEASE, be carefull and take every security measures possible.

Knowing that you can be see through CMD.exe running the Netstat -a command can also help you seeing if you're infected.

Use the command netstat -b , it will show you what file / .exe is using what connection, works as some sort of firewall with no option to block. :3

ALWAYS name your server some trusted windows file to "bypass" the curious eye. The most used filenames are: svchost.exe

explorer.exe

iexplorer.

taskmgr.exe [this one is my favourite]

TRICKS: You can change any .exe's extension to: .com [Name your file something like "pic102 @youremail@something" . Get it? :3]

.pif

.scr [Screen savers, this one also works fine for spreading]

.bat

You can also "spoof" your extension using a very well known public method. (You first will need to set the files to show extensions by going to Control Panel > Folder Options , look around and find something like : Show files extensions.)

Go to Start > RUN > Charmap > Now look for the character that will correspond to " U+202E : Left-To-Right overdrive" > Select it and copy > Go to your server , Right Click > Rename > Let's say your file is "image.exe". First add a space like this "image .exe". > Now paste the U+202E you just copied to right after the "e"> write the extension you want, BACKWARDS, like:3pm FOR mp3

gpj FOR jpg

xcod FOR docx

fdp FOR pdf

iva FOR avi

And so on and so on. You can choose ANY extension.

[FOR WINDOWS XP USER: Follow [THIS](#) tutorial here in order to install Unicode Characters so you can use this method!]

Some detection can be bypassed easily by just adding an HighRes Icon [Avira, sometimes] or a TRUSTED assembly like the HiJackThis program. To change an assembly or icon you can use : [ResourceHacker](#).

Thus ends our first week edition of: The RAT's Crew - Tips 'n Tricks.

CREDITSkill?Muvz: Design, Tip 'n Tricks, Crypters/undetected explanation, Security, Spreading.

Tibit: File Splitting TuT.

Untill next week,
Kill?Muvz

Lex - June 4, 2011, 8:32 am

Wow very nice "Guide". This will help a lot of members not only spreading there "RAT" but other things as well. Very detailed and easy guide to follow. Some things I haven;t thought of or seen before, So I will definitely need to try some of these out. Very nice Contribution to the community. Looks like you worked very hard on this. Looks like you have like a series you guys are doing Posting new stuff about Ratting ever week. I like it! Good Idea. Favorited this page just in case I decide to return to this.

Keep up the Good Work. ?

Kill?Muvz - June 4, 2011, 8:36 am

How kind, thank you alot for those nice words :3

People like you encourage me to keep working my arse off on thread like this :3

Portland Timbers - June 4, 2011, 8:38 am

I read the whole thing and it's very amazing. If you guys ever need help with these topics please send me a PM.

Blixx - June 4, 2011, 8:39 am

Another well done guide you made Killa. I missed nothing and i think everyone can work with this guide. I think there are many aspects that will help newbies and may some advanced ratters

RodasAPC - June 4, 2011, 8:41 am

Superb! I'd take your words over my teachers any day.

Azido - June 4, 2011, 8:43 am

Fantastic 'Tips 'n Tricks' guide.

5/5, loved it!

fodasse - June 4, 2011, 8:50 am

Always High Quality Tutoriais, High Qulity member Kilamuvz.

Always learning with RATS CREW.

Thanks Very much

Regards,

Kiksen - June 4, 2011, 8:54 am

rated 5 stars !! :D love this tut ! :D thnx mate ! :D

Kill?Muvz - June 4, 2011, 8:55 am

(Jun 4, 2011 08:43 AM)LIUZ Wrote: [\[CITE\]](#) Fantastic 'Tips 'n Tricks' guide.

5/5, loved it!

Why thank you! :3

Glad I'm helping lots of members!

Joey Tribbiani - June 4, 2011, 9:21 am

Correction - novirusthanks.org , not .com

Apart from that, this guide is pretty in-depth and well explained. I liked the ease of understanding factor.

Kill?Muvz - June 4, 2011, 9:32 am

Uh my bad, did that part in a hurry lol xD

Thanks brotato <3

prince.k94 - June 4, 2011, 9:49 am

This is one of the best informative tutorials on RATs. Keep up the good work. Can you give more information on PHP RAT. As my college network allows inwards connection through SSL-VPN only. So any slave can't contact me directly. That's why I want to use PHP RAT. Thanks in advance.

VoucherMaster - June 4, 2011, 9:51 am

I want to get into this crew. have been RATTING for a long time. When will you guys recruite?

Kill?Muvz - June 4, 2011, 10:21 am

I'm not sure :3 pm me your application, if you're good we will see.

Carb0n F1ber - June 4, 2011, 10:46 am

Another awesome thread. Thanks for the PM Killa :)

The best I liked in this is the hex editing. A very detailed noob-friendly one :)

Tibit - June 4, 2011, 11:23 am

Nice job Killa, if anyone has any questions about the HEX Editing message me, made the guide in a hurry so I might have made it hard to understand for some not used to it. Good job on the thread Killa.

Xycon - June 4, 2011, 11:32 am

seems the quality of "rats crew" has become better lately used to have some total noobs/retrats in it a few month ago
good to see changes

pippin - June 4, 2011, 11:45 am

Much respect to killaMuvz for taking his precious time out to put down this awesome tutorial. I will tune in next week most definitely.

VoucherMaster - June 4, 2011, 3:07 pm

Read both the tutorials. Nice and polished writing.

DaRkOoO - June 4, 2011, 3:37 pm

You can be caught even if you're not listening on ur client.

Server computer is trying to connect to client IP every x seconds, no matter if you're listening on client or not.

Kill?Muvz - June 5, 2011, 7:13 am

Not second. It's minutes, so it doesn't establish a connection, thus not making it an active one. So except the user uses a specific command to see every connection, even the closed ones he will not catch you. And to be honest if you're suspicious for an infection you'll not pay attention to closed connections.

(Jun 4, 2011 11:32 AM)Xycon Wrote: [\[CITE\]](#) seems the quality of "rats crew" has become better lately used to have some total noobs/retrats in it a few month ago
good to see changes

I'm here to prove the change :3

Tidas - June 5, 2011, 2:28 pm

What hex editor is that? You say that we can get the hex editor from a link and that link leads to the file splitter, not the hex editor. I don't see a hex editor link.

EDIT: Found it on Google. For all you peeps wondering, it's Hex Editor Neo.

EDIT again: Yes!!! FUD'ed my server! Thank god for you. Thank the frikken Lord for you.

Kill?Muvz - June 6, 2011, 9:22 am

No problemo brother :3

Cmon guys this is super detailed, read it :3

(Jun 4, 2011 09:49 AM)prince.k94 Wrote: [\[CITE\]](#) This is one of the best informative tutorials on

RATs. Keep up the good work. Can you give more information on PHP RAT. As my college network allows inwards connection through SSL-VPN only. So any slave can't contact me directly. That's why I want to use PHP RAT. Thanks in advance.

PM me. I'll give you everything you need.

Xenomorph™ - June 6, 2011, 1:20 pm

Very very HQ tutorial KillaMuvs.

Hope you guys keep up the good work.

?

Kill?Muvz - June 7, 2011, 1:39 pm

I will, don't worry :3

And thanks!

Burnzy - June 8, 2011, 6:25 am

[img]http://t2.gstatic.com/images?q=tbn:ANd9GcSq8TdngNHufwzAXLob05NH7dzJHEGcOJ_qjybn0i n0rT48iPQTTg[/img] for this thread, took alot of effort for this guide. and in rat's crew aswell.

SIM-701256 - June 8, 2011, 7:12 am

Extremly nice thread! lots of good information! :) i knew the most, but for beginners its an awesome guide :)

cyberzulu - June 8, 2011, 9:30 am

I love this guy hes very helpful

j.diesel - June 8, 2011, 10:12 am

very well done! super!! vouch for you man!!!!.pls keep it on and go deepr in next tutorial!

Kill?Muvz - June 9, 2011, 11:13 am

Well thank you!

Enjoy it.

01L 5P1LL - June 10, 2011, 2:09 pm

Well done killa..you make us all proud haha this one was really needed for everyone out there

Kill?Muvz - June 10, 2011, 2:34 pm

You're welcome. Glad you guys like it :3

Rwkeith - June 11, 2011, 7:23 am

Isn't changing the file extension more of a cosmetic thing? Does it effect the RAT at all....?

Tunasty - June 11, 2011, 8:10 am

This is an amazing guide. Very nice work done mate

Eshta - June 11, 2011, 10:20 am

Very nice

But....

Hex edit :

When i split my server and scan it no virus appears

any help ?

Boo. - June 11, 2011, 10:24 am

sniff sniff what's that smell? oh yeah, it's high quality. :) Great tutorial. Should PM Omni asking for free sticky.

Kill?Muvz - June 13, 2011, 5:22 am

If I PM him I just might get repfucked or smthing.

mashruwala - June 13, 2011, 7:19 am

My file get corrupt :(:(

Kill?Muvz - June 13, 2011, 7:49 am

Carefull on the Hex editing then.

mashruwala - June 13, 2011, 9:00 am

(Jun 13, 2011 07:49 AM)Kill?Muvz Wrote: [\[CITE\]](#) Carefull on the Hex editing then.I guess this technique doesn't work anymore ??

Kill?Muvz - June 13, 2011, 9:04 am

It does, it can't be "patched". Just be carefull on what you edit.

Water Antilope - June 13, 2011, 9:09 am

great tut man very detailed thanks for writing this man

mashruwala - June 13, 2011, 9:15 am

(Jun 13, 2011 09:04 AM)Kill?Muvz Wrote: [\[CITE\]](#) It does, it can't be "patched". Just be carefull on what you edit.

Even if I change the alphabet it doesnt work for me it gets corrupt :(

And ya In the TUT there is 1 photo missing "hex section"

Glaedr - June 13, 2011, 10:13 am

Cool tutorial. I am looking forward to see the next episode:)

DerHeXxXer - June 13, 2011, 10:30 am

cool tut mate ;)

btw, the pics of stub and file are taken out of the blueprint ebook, arent they?

Pebis - June 13, 2011, 11:27 pm

Thanks alot for this i needed some sources xD

VeLo - June 13, 2011, 11:54 pm

Bookmarked this weeks Tips and Tricks as well as the last one. Nice work! :D

SirKiller - June 14, 2011, 2:10 am

thanks man , that really helped

Boo. - June 14, 2011, 2:20 am

Thanks for the trick. I just tried it and it looks amazing.

rahan - June 14, 2011, 3:12 am

I did not try to make any virus but i found other useful things in you tutorial.Thanks very much

Kill?Muvz - June 14, 2011, 5:42 am

(Jun 14, 2011 02:20 AM)Club Wrote: [\[CITE\]](#) Thanks for the trick. I just tried it and it looks amazing. You're welcome :3 Unfortunatly It was not possible to do a last weeks edition, as I'm extremely busy with exams and I should be studying harder.

(REATOR - June 15, 2011, 2:38 am

Awesome tutorial.Hats off to rat's crew.Never saw a better tutorial(I am not ass kissing but telling my opinion).You guys really put a lot of effort into writing tutorials.Thanks a ton..!

Kill?Muvz - June 15, 2011, 5:29 am

(Jun 15, 2011 02:38 AM)(REATOR Wrote: [\[CITE\]](#) Awesome tutorial.Hats off to rat's crew.Never saw a better tutorial(I am not ass kissing but telling my opinion).You guys really put a lot of effort into writing tutorials.Thanks a ton..!

This one took more way more then 12 hours :3

Thank you sir, enjoy !

Hacder - June 15, 2011, 4:23 pm

Awesome man, if you see my new posts/threads, you'll know how noob i am with RATs stuffs until now, but after reading your thread, i got so much knowledge i couldn't get in so short time, +1 rep'd for so damn HQ tut, thanks a lot mate, i really liked it :)

Kill?Muvz - June 17, 2011, 5:02 am

Lol thanks bro. Glad I helped.

manele2011 - June 17, 2011, 5:07 am

When is the next week (week number 3) ?:D

thanks

Kill?Muvz - June 17, 2011, 6:07 am

When I get time. I'm extremely busy =x

Morbid Saint - June 17, 2011, 6:36 am

Very nice guide, it will help lots of people to understand how all those things work. Thanks. :)

Kill?Muvz - June 18, 2011, 3:15 pm

Thanks alot, I'm glad you like it.

Enjoy it!

Iars90 - June 18, 2011, 5:06 pm

hey edditing does not rally work anymore i can make a file undetected by 3 less AV systems no more though

Kill?Muvz - June 19, 2011, 5:36 am

You're doing it wrong then :3 It will work forever..

CharleyisHere1 - June 19, 2011, 7:43 am

Very nice and helpful tutorial. I used some of your techniques.

Kill?Muvz - June 20, 2011, 10:17 am

You're welcome. Enjoy it! :3

C??????? - June 20, 2011, 11:02 pm

Nice,.. Great Tut Again :)

Kill?Muvz - June 21, 2011, 12:49 pm

Thanks bro. Enjoy it!

BUMP

Huckzy - June 21, 2011, 2:18 pm

This is simply Brilliant! One of the best Tutorials, Tips & Tricks etc here on HF. Great thread!

Thank you so much for taking time to write this. ?

Kill?Muvz - June 21, 2011, 2:29 pm

It did take a lot of work to write it. But thank you, it was with the sole purpose to teach :3

Tidas - June 21, 2011, 5:09 pm

Hex Editing corrupts my server, what do? There's not much I can change because they have strange characters in them and I tried all the ones where I can just capitalize or make something lowercase.

Golliath808 - June 22, 2011, 4:36 am

(Jun 21, 2011 05:09 PM)FridgeFry Wrote: [\[CITE\]](#) Hex Editing corrupts my server, what do? There's not much I can change because they have strange characters in them and I tried all the ones where I can just capitalize or make something lowercase.

Surely will corrupt your server sometimes, or if you change whole code. just try try and try and slowly.

Now for the OP:

Great tuts especial for begginers, damn, they have alot of learning in the skillz of RATting :P . How about posting in the security section something about the Blackshades station ?? Is that good way to be more anonymous?

EDIT: and the correct extension is " pif " not piff.

Kill?Muvz - June 22, 2011, 4:45 am

(Jun 22, 2011 04:36 AM)Golliath808 Wrote: [\[CITE\]](#) Surely will corrupt your server sometimes, or if you change whole code. just try try and try and slowly.

Now for the OP:

Great tuts especial for begginers, damn, they have alot of learning in the skillz of RATting :P . How about posting in the security section something about the Blackshades station ?? Is that good way to be more anonymous?

EDIT: and the correct extension is " pif " not piff.

I'll take a look @ the bshades thing :3

Glad you like it.

Oh and thank you.

Burnzy - June 22, 2011, 8:02 am

bu.mp! This one too. Glad you guys like it!

1c3y - June 22, 2011, 10:55 am

Props to you and anyone else who helped make this guide, really helpful and detailed. Thanks

Kill?Muvz - June 22, 2011, 11:01 am

Thanks 1c3y :3 glad you like it.

Lemonade - June 22, 2011, 11:23 am

After reading this I must say it is fantastic and I hope it helps many members.

Kill?Muvz - June 22, 2011, 11:30 am

Well thank you. Glad you like it.

KoD™ - June 25, 2011, 4:45 am

I'm glad I got into this crew, it's so much helpfull threads here :)

m4dh4ck3r - June 25, 2011, 5:09 am

THE BEST TUT EVER !

Going to try the crypting with file splitter !

Hope it works !

Thanks :)

lithis - June 25, 2011, 6:48 am

I never even knew about the hex editor, I'm going to try it.

EDIT: Both avira and MBAM come clean for the 4 parts... odd.

EDIT 2: Would we be able to use VT for splitting/hexing? I mean, not showing the changed file just narrowing down which is the signature.

Man when I see stuff like this after not going into the RATs and hacks section for weeks, I really love it.

I actually thought the RAT crew were just a bunch of people socializing, obviously i was wrong, glad I was.

Really HQ, wish I could +3 rep.

Kill?Muvz - July 1, 2011, 2:26 am

That means you just split the line that contained the detection.

jimply - July 1, 2011, 8:20 am

Verry nice guide thanks! this will be usefull!

HITMANCCC (dirty version) - July 2, 2011, 1:37 pm

No One Really WOuld Trace You So Dont mater And Dynamic Ip

Pebis - July 2, 2011, 2:00 pm

Thanks for all of this. ?

oolegitoo - July 2, 2011, 2:16 pm

Thanks for the help!Helped me very much!!!??

engtmk - July 2, 2011, 3:48 pm

Real good and informative.

lot of great details in simple manner.

Kill?Muvz - July 4, 2011, 3:34 am

(Jul 2, 2011 01:37 PM)HITMANCCC (dirty version) Wrote: [\[CITE\]](#) No One Really WOuld Trace You So Dont mater And Dynamic Ip
You sure? I've SEEN people trying to trace me.

Zachu24 - July 4, 2011, 3:50 am

Great tips man! looking foward to more tips!

Golliath808 - July 4, 2011, 1:08 pm

When do you will launch a W33K 3 Tip's and tricks ;) ??

Kill?Muvz - July 4, 2011, 2:00 pm

Next edition will be a MASSIVE one, reason for taking so long.

-=SaGaR=- - July 4, 2011, 2:02 pm

(Jul 4, 2011 02:00 PM)Kill?Muvz Wrote: [\[CITE\]](#) Next edition will be a MASSIVE one, reason for taking so long.

Based on which topic? ?

Animation - July 4, 2011, 2:08 pm

Nice guide well written and gave tips anyone could use beginner or not!

mane1e2011 - July 5, 2011, 1:55 am

(Jul 4, 2011 02:00 PM)Kill?Muvz Wrote: [\[CITE\]](#) Next edition will be a MASSIVE one, reason for taking so long.

Awesome man!!! i'm so excited. i can't wait for itt :X:X:X

respect ?

Carb0n F1ber - July 5, 2011, 2:02 am

(Jul 4, 2011 02:00 PM)Kill?Muvz Wrote: [\[CITE\]](#) Next edition will be a MASSIVE one, reason for taking so long.

And I was just going through all your posted threads to see if I missed something. Awesome, looking forward ?

Kill?Muvz - July 8, 2011, 7:56 am

(Jul 5, 2011 02:02 AM)Carb0n F1ber Wrote: [\[CITE\]](#) And I was just going through all your posted threads to see if I missed something. Awesome, looking forward ?

Dun worry, like I did before I'll let you know when a new one comes out.

cancrusher - July 12, 2011, 10:08 am

all i can say is WOW!!!!,been trying to understand all about RATS by reading other threads,then i came across this one..and its so well written and easy to understand,its made life so much easier....kudos to you dude.

punk5555 - July 12, 2011, 10:43 am

ver nice post...awesome...perfect for a noob to understand the vocab used...thanks!

Burnzy - July 16, 2011, 2:46 am

bu.mp cuz i see dumb threads rat's crew dont give a fuck to help here.

?us?ness - July 16, 2011, 2:53 am

Another great thread from the RAT's Crew :)

Kill?Muvz - July 16, 2011, 6:47 am

Yep. Bump for this. Great for newbies.

AlooshXD - August 24, 2011, 12:11 am

wow this is really amazing thread O.O !

Kill?Muvz - September 16, 2011, 3:59 pm

Read it newbies, you'll find it really helpfull!

Tamrock - September 16, 2011, 7:49 pm

This was very interesting, thanks alot!

Good work.

ahmadludin - September 25, 2011, 6:11 pm

im a newb and man reading that confused me like crazy. would you please just cript my server.exe?
please

M4C - October 7, 2011, 12:03 am

Awesome thread, very informational ;]

Kill?Muvz - October 7, 2011, 4:50 am

Thanks. If everyone read the whole series there wouldn't be so many junk there.

bsquidwrld - October 15, 2011, 4:02 am

Thanks for this post OP! I really appreciate you taking the time to create such a HQ and informative post. Definitely bookmarking for later too ^_^

kaviya1 - October 15, 2011, 9:19 am

tnx a lot man for this nice tut

hope the next one will come soon ?

Kill?Muvz - November 2, 2011, 11:04 am

You're welcome. I'm thinking on making another edition, what do you guys think?

treadmill - November 5, 2011, 5:32 am

Go for it!!

The first three are superb.

FuriousHawk - November 5, 2011, 8:38 am

This is the most interesting post i've ever seen in this subforum !!

Great job explaining Stub,USG,... !!

arti456 - November 9, 2011, 11:23 am

great tutorial man.... but in your File undetection / encryption section under Hex editing images are not displaying.... kindly update

Old Days - December 29, 2011, 12:09 pm

You've enlightened me with lots of knowledge by this useful tutorial. Thank you for sharing.

Regards.

PS: Is it possible to change the icon of file of .com extension permanently, that even if I move that file to another PC then that server.com file will have that same changed icon in other PCs?
Is that possible or not?

superkidhj - January 3, 2012, 4:55 am

Thanks for the great guide. Keep it up bro. :)

Prominent - January 3, 2012, 7:24 am

Well done The RAT's Crew, I see a lot of effort put into this. ;)

Bonds - January 3, 2012, 2:00 pm

Hey, I was wondering if someone can help me.

I have set up DarkComet correctly but I need someone who is willing to test it for me (as testing it on myself with 127.0.0.1 isn't effective on testing whether it works on someone else). Here's what I have done so far:

- Port Forwarded (port shows up as open on canyouseeme.org)
- DarkComet settings set up correctly and as shown in several tutorials
- No-IP and DUC set up
- Crypted about a week ago but the stub is beginning to show as detected on several AV's, will re-crypt with a new stub as soon as I know it works on others.

All I need is someone who is willing to test this for me. We can TV the entire time, etc. I'm not looking to infect anyone on this site ever. Thank you!

United States of America - January 3, 2012, 2:22 pm

"Using PHP R.A.T.'s. Why? Well read the previous week edition and you'll see that PHP R.A.T.'s do not connect directly, therefore your IP will not be visible to netstat or any other method."

Can't say I knew that :P. Nice guide man! Thanks a lot!

hopptramp - January 22, 2012, 11:43 am

Thanks for a great tut! Muy useful. Keep it up :)

FuhrerWulf - January 30, 2012, 6:41 am

Very well done and very helpful thread rats crew ?

Salvatore - January 30, 2012, 8:53 am

Wow. This was really helpful! Really appreciate the time you took to write this. Love it, great job.

TheFeed - February 8, 2012, 10:40 pm

Both this and your first thread are very well done ...

Appreciate the efforts ~!~

Cedric. - February 14, 2012, 1:46 pm

It's completely clear for me how this works thank you for this threads!. to bad I don't have the balls to

try this. I'm to scared to do things with my router and getting caught etc.

xhelmi - February 19, 2012, 6:49 am

Very nice and usefull Tuts... Easy to understand

Well done

Lady Deathstroke - February 19, 2012, 6:55 am

really good thread once again would also rate it 5/5 i think i learned a bit reading your post thanks once again rat crew

Andy Sharma massacre - April 20, 2012, 9:53 am

Thank you very much
helped me alot:)

Keroyugi - October 15, 2012, 2:02 am

and it's getting better, hope i see better in the next thread.

Kozey11 - March 12, 2013, 9:36 pm

i need help with this, but im not allowed to send PM's yet:(

back5 - March 12, 2013, 9:51 pm

this is now bookmarked, thank you so much for this. I wanted to know how to re-FUD the stub but I could never find anything. this will be a good starting point for me in that area (Y)