

Forum:[Hack Forums](#)

Thread: [\[TuT\]how does crypter work \[everything explained\]](#)

Burnzy - July 26, 2011, 4:58 am

[img]http://img16.imageshack.us/img16/3444/inactivitybanner.png[/img]

this info is from RAT's crew tips and tricks week #2 which can be found [here](#) i just extracted it so you guys can bookmark this thread and learn much more about crypters credits for the tut goes to RC leader killamuvz and others who helped <3

also check out [The RAT's Crew tips n' tricks week #3](#)

Check out!!!

[Cryptex crypter!!](#)

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 it Fully Un-Detectable for a period of time?

That's why there are these freaky tools that do things beginners 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.

Runtime : This is the most common, and loads of free crypters only are Runtime FUD. Meaning they are undetectable while running the PC normally 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. If a crypter says RunPE somewhere it means it is Runtime

Or both. If you're planning on buying a Crypter make sure it is 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 Crypter 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:

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 than 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 slave 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 slave 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 basicly: File Spliting + 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 accused 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!

Ton33y - July 26, 2011, 5:00 am

Awesome guide man! Explained everything I needed to know about crypters!

Get Hit - July 26, 2011, 5:03 am

i love the tut mate nice good

devilpsn - July 26, 2011, 5:03 am

Nice Guide I saw some of the same information in the crypter's blue print by xinifltrate

Burnzy - July 26, 2011, 5:07 am

you gotta love this one, hope the next week will be soon, i think we're out of ideas.

Glype - July 26, 2011, 5:22 am

Nice tut mate. very well explained

Unkraft - July 26, 2011, 5:29 am

Nice tut man, still need a lot of time to master this fud rat **

rip2444 - July 26, 2011, 6:03 am

Nice tutorial.... i was wondering what the heck Stub.exe was...

Burnzy - July 26, 2011, 6:10 am

yeah, you see that word alot, good to know what does it means.

Nathan Moriarty - July 26, 2011, 7:16 am

(Jul 26, 2011 04:58 AM)Ray William Johnson Wrote: [\[CITE\]](#) 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.

I don't see the difference between 'fully undetected' and 'undetected'. Can someone explain?

BloodFire - July 26, 2011, 7:22 am

(Jul 26, 2011 07:16 AM)nateepie Wrote: [\[CITE\]](#) I don't see the difference between 'fully undetected' and 'detected'. Can someone explain?

~_~ fully undetected is when you crypt a virus and it is fully undetected by any type of anti-virus/spyware like when you scan and the result is 0/33 that is called FUD.

un-detected is when you crypt a virus and some anti-virus/spyware detect them and some don't. Example when you scan and the result is 3/33 that means it is just UD not FUD.

Nathan Moriarty - July 26, 2011, 7:36 am

(Jul 26, 2011 07:22 AM)BloodFire Wrote: [\[CITE\]](#) ~_~ fully undetected is when you crypt a virus and it is fully undetected by any type of anti-virus/spyware like when you scan and the result is 0/33 that is called FUD.

un-detected is when you crypt a virus and some anti-virus/spyware detect them and some don't. Example when you scan and the result is 3/33 that means it is just UD not FUD.

I don't see how that is possible. Let's say my grandma was completely (fully) dead. Then non of her inner organs would be functional (ex. 0/33), and again, if she was dead it would be same outcome; 0 operative organs.

SHORT: Dead = Fully dead, either your dead or your not. Not just a little dead.

bobby2 - July 26, 2011, 8:01 am

Nice TuT, Very well explained about File Split + Hex Editing to FUD the Server

Burnzy - July 26, 2011, 9:32 am

(Jul 26, 2011 07:36 AM)nateepie Wrote: [\[CITE\]](#) I don't see how that is possible. Let's say my grandma was completely (fully) dead. Then non of her inner organs would be functional (ex. 0/33), and again, if she was dead it would be same outcome; 0 operative organs.

SHORT: Dead = Fully dead, either your dead or your not. Not just a little dead.

triple ? do you even know what av is how many of them exists and how do they work?know what av is how many of them exists and how do they work?

Nathan Moriarty - July 26, 2011, 9:37 am

(Jul 26, 2011 08:09 AM)Ray William Johnson Wrote: [\[CITE\]](#) triple ? do you even know what av is how many of them exists and how do they work?know what av is how many of them exists and how do they work?

I didn't completely understand what you are trying to say. Correct me if I'm wrong; You're asking if I know what an antivirus is, how many antivirus programs exists, and how they work? Which isn't relevant to my original assertion. Quote fail?

I can try to rewrite my statement in a more understandable way; 'Fully undetected' = 'undetected'. It's like an ON/OFF switch, its either undetected or detected.

GiGz - July 26, 2011, 11:44 am

Is that thr real RWJ?!?!?

Burnzy - July 26, 2011, 11:44 am

But when it's ud 1 or MORE

THAN 1 AV WILL PICK IT UP.

Let's say your server is detected

by avira antivirus

that means ur server is ud

and if your target has avira

installed you wont be able to
infect him while others who
doesn't have avira WILL GET
INFECTED.

happy now?

(Jul 26, 2011 11:44 AM)GIGLOGAMINO Wrote: [\[CITE\]](#) Is that thr real RWJ!?!?

yes it is :) ?

am ray william johnson and i approve this message.

Nathan Moriarty - July 26, 2011, 12:09 pm

(Jul 26, 2011 11:44 AM)Ray William Johnson Wrote: [\[CITE\]](#) But when it's ud 1 or MORE
THAN 1 AV WILL PICK IT UP.

Let's say your server is detected

by avira antivirus

that means ur server is ud

and if your target has avira

installed you wont be able to

infect him while others who

doesn't have avira WILL GET

INFECTED.

happy now?

No. So you're saying that if 1 antivirus detects a virus then the virus is undetected? You see why
that doesn't make sens?

Burnzy - July 26, 2011, 12:15 pm

use logic bro.

If antivirus detects it that means it's ud or not ud at all.

If it doesn't get detected by any av then it's fud!

Damn.

Nathan Moriarty - July 26, 2011, 12:34 pm

(Jul 26, 2011 12:15 PM)Ray William Johnson Wrote: [\[CITE\]](#) use logic bro.???

(Jul 26, 2011 12:15 PM)Ray William Johnson Wrote: [\[CITE\]](#) If antivirus detects it that means it's ud
or not ud at all.What? If a antivirus detects a virus its undetected or not undetected? That didn't
make sens.

(Jul 26, 2011 12:15 PM)Ray William Johnson Wrote: [\[CITE\]](#) If it doesn't get detected by any av then
it's fud!Yes, I agree. FUD = Fully undetected, which is the same as undetected.

Burnzy - July 26, 2011, 3:40 pm

you know what? When i swich to

pc i'll open a ms paint and draw

you it!

Fuck!

Nathan Moriarty - July 26, 2011, 5:17 pm

(Jul 26, 2011 03:40 PM)Ray William Johnson Wrote: [\[CITE\]](#) you know what? When i swich to

pc i'll open a ms paint and draw

you it!

Fuck!

I am a pretty smart guy (144 IQ, official test) and I don't see how something that is undetected can

be detected. I might be wrong, but I don't see the logics you mentioned earlier.

Slash - July 26, 2011, 8:13 pm

Thakyou so much..That really helped me learn a lot about crypters...Thankyou !!

Slash - July 26, 2011, 8:13 pm

Thakyou so much..That really helped me learn a lot about crypters...Thankyou !!

Burnzy - July 27, 2011, 1:34 am

(Jul 26, 2011 05:17 PM)nateepie Wrote: [\[CITE\]](#) I am a pretty smart guy (144 IQ, official test) and I don't see how something that is undetected can be detected. I might be wrong, but I don't see the logics you mentioned earlier.

then prove it lol... I knew what's fud and what's ud when i first time heard about rat.

Nathan Moriarty - July 27, 2011, 1:55 am

(Jul 27, 2011 01:34 AM)Ray William Johnson Wrote: [\[CITE\]](#) then prove it lol... I knew what's fud and what's ud when i heard about rat first time.

That's what I've done since the beginning. It's you who need to prove me wrong.

h4kr! - August 10, 2011, 4:08 am

looks like it would be good if i knew what

"..IData..."was or even worse:

"ÄÖýðCdž?nN"

:(

Rvaveo - August 10, 2011, 4:28 am

(Jul 26, 2011 05:17 PM)nateepie Wrote: [\[CITE\]](#) I am a pretty smart guy (144 IQ, official test) and I don't see how something that is undetected can be detected. I might be wrong, but I don't see the logics you mentioned earlier.

Well you are right but people just call it ud.So you can't do anything about it.?

spikebites - August 10, 2011, 4:40 am

(Aug 10, 2011 04:28 AM)Ultimate Coder Wrote: [\[CITE\]](#) Well you are right but people just call it ud.So you can't do anything about it.?

it's like this... sometimes my penis is hard.... but, other times, my penis is ROCK HARD... get it?... UD and FUD?.. same thing.

BloodFire - August 10, 2011, 4:58 am

(Jul 26, 2011 05:17 PM)nateepie Wrote: [\[CITE\]](#) I am a pretty smart guy (144 IQ, official test) and I don't see how something that is undetected can be detected. I might be wrong, but I don't see the logics you mentioned earlier.

you have a point but your 144 IQ lacks in common sense IMO because if you put common sense in it then you'll just have to assume that what they mean in UD or undetected is "undetected by other anti-virus" and they're just wrong about the term.

Vexna - August 10, 2011, 5:15 am

Good work, very well explained. I miss RTC :3

BtK - August 10, 2011, 6:17 am

i have some questions:

let's say that i crypt my server with an unique stub crypter and i don't spread it but i use it only with

1-2 people that will not check the file on virustotal... this means that my RAT will last forever?

binding : can i do it before crypting? or it's better after?

startup : what's the difference between start only server or start crypted file?

InZanitY - August 10, 2011, 6:29 am

Thanx for the tut, learned a few new things!

BloodFire - August 10, 2011, 6:53 am

(Aug 10, 2011 06:17 AM)_BtK_ Wrote: [\[CITE\]](#) i have some questions:

let's say that i crypt my server with an unique stub crypter and i don't spread it but i use it only with 1-2 people that will not check the file on virustotal... this means that my RAT will last forever? I think not, it will last long but I think not forever.

Quote:binding : can i do it before crypting? or it's better after?

its always good to bind it first then crypt it. specially if your binder is not FUD.

Quote:startup : what's the difference between start only server or start crypted file?

I'm confused here do you mean the difference between RAT startup and crypter startup? If so, I think the custom installation and registry . because some crypter registry and installation is not customizable there for you cannot hide your RAT properly.

Mr. Wallstreet - August 10, 2011, 7:36 am

nice tut i actually read the whole thing ^.^

BtK - August 10, 2011, 7:43 am

(Aug 10, 2011 06:53 AM)BloodFire Wrote: [\[CITE\]](#) I think not, it will last long but I think not forever. well, i don't mean really forever... what's typically the duration for a good crypter? 3-4 weeks? if i don't spread it it could last some months?

(Aug 10, 2011 06:53 AM)BloodFire Wrote: [\[CITE\]](#) its always good to bind it first then crypt it. specially if your binder is not FUD.

so also the binder should be FUD? in this case maybe it's better to find a crypter that has also a binder feature...

(Aug 10, 2011 06:53 AM)BloodFire Wrote: [\[CITE\]](#) I'm confused here do you mean the difference between RAT startup and crypter startup? If so, I think the custom installation and registry . because some crypter registry and installation is not customizable there for you cannot hide your RAT properly.

yes, i meant the difference the RAT startup and crypter startup 'cause i see many crypter have this option...

maybe i don't get it, but i understood that a crypted file at the startup is decrypted so it means that it becomes virtually detectable... so why should i prefer to startup the crypted one instead of the RAT pure and simple?

grrga - August 10, 2011, 7:46 am

Thnx, man, if u can tell some book of crypting for download or PM?

BloodFire - August 10, 2011, 8:36 am

(Aug 10, 2011 07:43 AM)_BtK_ Wrote: [\[CITE\]](#) well, i don't mean really forever... what's typically the duration for a good crypter? 3-4 weeks? if i don't spread it it could last some months? 2-3 months or

more I think specially if he used a private crypting method.

Quote:so also the binder should be FUD? in this case maybe it's better to find a crypter that has also a binder feature...

yes it has to be fud. because binding is illegal to some anti virus. so yes its better to have a crypter with a binder in it^^

Quote:yes, i meant the difference the RAT startup and crypter startup 'cause i see many crypter have this option...

maybe i don't get it, but i understood that a crypted file at the startup is decrypted so it means that it becomes virtually detectable... so why should i prefer to startup the crypted one instead of the RAT pure and simple?

If you crypt your server either of the two startup will be undetected by the computers anti virus.

so it will depend on the scenario because some crypters corrupts the RAT startup option there for you have no choice but to use the crypter startup. and some other crypter has a startup persistence feature, surely you would pick the crypter startup if thats the case. and some crypter has no startup option there for you'll just have to use the rats startup option.

its just about common sense. If you think you'll have more advantage in the crypters startup then go for the crypters startup.

and if you think the crypters startup sucks because its not customizable then use the RAT's startup option.

and tip: don't use two startup option at the same time. if you're gonna use the RAT's startup make sure to disable the crypters startup option.

Rvaveo - August 10, 2011, 9:23 am

(Aug 10, 2011 04:40 AM)t('t) Wrote: [CITEI](#) it's like this... sometimes my penis is hard.... but, other times, my penis is ROCK HARD... get it?... UD and FUD?.. same thing.

No i don't understand it that way.lol.

Burnzy - August 10, 2011, 10:18 am

lol then dont even try to understand...

Burnzy - September 2, 2011, 1:48 pm

bu.mp, alot of effort has been invested here, hope you guys who didn't see it yet like it:)

heggan - September 2, 2011, 2:01 pm

hmm nice tutorial, btw that split+hex methode works for all kinds of servers right?

sseagal - September 2, 2011, 2:12 pm

can there be done an ultimate cryper? like that it would encrypt the whole files(an all added later) with a strong encryption(like aes, or maybe some combined rsa) of a long key. So that everytime installed, all its files would be everytime unique(depending on the key) and to communicate with the encrypted rat a succesful key entry would have to be made first(rat only acting as reciever until succesful key entry was made to a specific random process(that would be changing frequently(maybe based on the recent system actions))). i'm on to it, cose i made my first program today :D, so nothing can stop me now lol

forgot to thank for the thread :), thanks, another step forward(if used wisely ofc :)

edit: and maybe the crypter could use more different keys, to make a backups of himself in case found and disabled, some system restore ms-like feature.

porndude99 - September 2, 2011, 5:21 pm

thank you for this, very informative

Burnzy - September 3, 2011, 2:48 am

god damn some images are broken ._. will try to fix.

CharleyisHere1 - September 4, 2011, 4:37 am

Thanks for this one. Very informative.

hippy01 - September 5, 2011, 5:25 am

thx for this post very helpfull much appreciated

Idle cares - September 5, 2011, 5:33 am

Thanks for this informative article :) I've learnt from it.

rapidfire08 - September 11, 2011, 1:50 am

Wow This Tut is so amazing thanks for the information :)

cbirdicus - September 14, 2011, 8:54 pm

Thanks for the information. This really cleared up questions I had about crypting :D

WHITE-sOUL - September 15, 2011, 3:41 am

this a very nice guide thanks a lot.

WS

only4u - September 18, 2011, 11:42 am

lulz lulz wot?... omfg-?

Ive saw this another place , b4 l???

this is leaked! for shure ehm

froshroom - September 19, 2011, 10:01 am

Thanks for making a great tutorial, very clear and concise.

franzzz - September 19, 2011, 11:13 am

Awesome guide! :) Explained every detail very well.

Burnzy - September 19, 2011, 12:32 pm

thanks for positive feedback guys! Killa and others who made this appreciate it for sure.

carl020989 - September 19, 2011, 1:01 pm

Very informal, nice tutorial. Good job; thanks. :)

exalted - September 19, 2011, 2:38 pm

Thanks alot, this could help me understand how a crypter is built up :)

BBall Star - September 19, 2011, 3:30 pm

This thread was Copy and Pasted from The Crypter Blueprint, you even put the pictures from it too.

Please put this in the Original Thread.

Burnzy - September 19, 2011, 11:59 pm

(Sep 19, 2011 03:30 PM)Mafia Wrote: [\[CITE\]](#) This thread was Copy and Pasted from The Crypter Blueprint, you even put the pictures from it too. Please put this in the Original Thread.

read the start of a thread num nut, rat's crew members did this, i linked to original thread.
LoLBrouBlind

B3cnoc - September 20, 2011, 6:54 am

Great tutorial for people who don't know about crypters. Thanks for sharing your good work.

HakkuR - September 20, 2011, 7:10 am

.NET Framework is extremely powerful and is underestimated as "bad coding for malware", it is taking over the PC world slowly and all computers will have it.

mr spud - September 21, 2011, 4:11 pm

Nice explanation. Helped me a lot. :P

Burnzy - November 5, 2011, 10:32 am

bu.mp for a hard work and proof of trc high quality :)

Java Coder - January 6, 2012, 2:27 am

This is amazing, thanks a whole lot! It helped me understand all of this a lot more.

sean3200 - January 21, 2012, 6:07 pm

hey why cant i see pics :(... i only see the text and a link that says spoiler with a image text thats it..
plzz help

Almightylove - January 29, 2012, 6:09 am

Good tutorial :) well explained it will help me alot

KingKratom - January 29, 2012, 7:00 am

Thanks this really helped are paid crypters both runtime and scantime?
i have chronic crypter

rpasswords - February 2, 2012, 2:40 am

This is Perfect. Just what i needed. Thanks for sharing

Burnzy - October 12, 2012, 1:13 pm

ing this thread in a memory of The RAT's crew which i was a part of since 2010