

Forum:[Hack Forums](#)

Thread: [Confused About Crypt-Rat Install Chain](#)

Crazy Ralph - October 31, 2012, 11:27 pm

Ok, I am (admittedly) confused when trying to understand how the crypter interacts with the original RAT server file. I have this feeling that it 'covers' the original file and doesn't adopt the properties of the original file...but I am not so sure.

So, here is my question:

When you crypt a server file to make it FUD, when that file is opened by a slave, does the encryption allow the server file to pass through the AV layer, then self destruct and leave the original server file to do it's thing?

Example: if you were to chose 'melt' and 'add to startup' in the crypter settings, is that referring to the crypted layer and not the original server file or does choosing 'melt' and 'add to startup' make the original server file melt and added to startup?

Man, I don't feel like I am explaining this well, at all.

Um...

Does the original server file become an entirely NEW file that combines it's properties and the encryption as well or are they still two distinctly different files that are combined to join forces?

G'damn, if I could just understand this then I would know exactly what settings to use in building the RAT server file and then in the crypter.

Does anybody know what I am talking about or am I just as insane as my screen name suggests?

Assault - November 1, 2012, 4:50 am

The RAT's bytes encrypted & stored into a stub that the crypter outputs.

From there, at runtime the stub will decrypt those bytes & run them in the memory.

? ?nfinity ? - November 1, 2012, 5:03 am

(Nov 1, 2012 04:50 AM)Assault Wrote: [\[CITE\]](#) The RAT's bytes encrypted & stored into a stub that the crypter outputs.

From there, at runtime the stub will decrypt those bytes & run them in the memory. Exactly what he said, a Crypter encrypts all bytes from the actual server, on runtime all those bytes will be decrypted in the memory.

The file will still remain the same, just the bytes which are encrypted.

Fifa 13 - November 1, 2012, 5:44 am

I got the same problem!

Will check this thead l8 and hope someone has find a solution.

Assault - November 1, 2012, 6:25 am

(Nov 1, 2012 05:44 AM)Lahe Wrote: [\[CITE\]](#) I got the same problem!

Will check this thread and hope someone has found a solution.
What problem..? The OP didn't say anything.

Kimia - November 1, 2012, 6:39 am

Here is my simple explanation.

File A = is our crypted rat. Let us assume someone downloaded it.

Startup function?

When the person runs your "File A" it will copy itself to some folder in the computer (we can name the new file as "file B")

File A is totally same with File B, maybe the difference is only the name.

File B will be run everytime the slave computer restarts.

Melt function?

When the person runs your "file A", it will do all the job above and delete itself at the last process.

? ?nfinity ? - November 1, 2012, 6:52 am

(Nov 1, 2012 06:39 AM)Kimia Wrote: [\[CITE\]](#) Here is my simple explanation.

File A = is our crypted rat. Let us assume someone downloaded it.

Startup function?

When the person runs your "File A" it will copy itself to some folder in the computer (we can name the new file as "file B")

File A is totally same with File B, maybe the difference is only the name.

File B will be run everytime the slave computer restarts.

Melt function?

When the person runs your "file A", it will do all the job above and delete itself at the last process.
No you are not right.

Startup would simply add a registry value so it would startup everytime windows would start.
It wouldn't make a new file.

And the melt function just hides the files A.K.A. making it invisible, it will not be deleted.

Crazy Ralph - November 1, 2012, 8:39 am

So, if the crypter is of good quality then there is little or no need to select melt, persistence, or startup options when making the server file? That if I select 'melt' and 'startup' during encryption, those options will stay with the file until....well, until the file is dead?

? ?nfinity ? - November 1, 2012, 8:42 am

(Nov 1, 2012 08:39 AM)Crazy Ralph Wrote: [\[CITE\]](#) So, if the crypter is of good quality then there is little or no need to select melt, persistence, or startup options when making the server file? That if I select 'melt' and 'startup' during encryption, those options will stay with the file until....well, until the file is dead? I wouldn't recommend melt, when the slave runs the file it would immediately disappear which is really suspicious IMO.

Startup and persistence should be selected though, without startup the slave would disappear when he restarts his computer and persistence makes it harder to remove the file.

Crazy Ralph - November 1, 2012, 8:47 am

(Nov 1, 2012 08:42 AM)glnxhjih Wrote: [\[CITE\]](#) Start up and persistence should be selected though, without start up the slave would dissapear when he restarts his computer and persistence makes it harder to remove the file.

I am using DP (Data Protector) and it doesn't have a persistence option, only startup. Would it be a good idea for me to select 'persistence' in DC when I am building my server file or would that corrupt the file after it's crypted? Thanks for your help, by the way. Damn, it's nice to figure this stuff out ?

BoomShot - November 1, 2012, 9:45 am

It'd most likely corrupt the file, but you can try it on yourself if you want. You'll know it's corrupt if you get an error or you don't infect yourself.

northman - November 1, 2012, 10:26 am

You've had DataProtector for around a month at least Crazy Ralph, If you still haven't figured out how to use it pm me and I will show you exactly how to set everything up with your Rat step by step.

Crazy Ralph - November 1, 2012, 11:56 am

(Nov 1, 2012 10:26 AM)northman Wrote: [\[CITE\]](#) You've had DataProtector for around a month at least Crazy Ralph, If you still haven't figured out how to use it pm me and I will show you exactly how to set everything up with your Rat step by step.

Ok cool. Thanks. I appreciate it, northman.