

Forum:[Hack Forums](#)

Thread: [So FTP RATs Aren't A Thing?](#)

TerminallyIII - December 22, 2018, 8:02 pm

Looking at some posts here I noticed that people don't really consider FTP RATs a thing. Has a RAT that uses FTP as a C&C server ever existed? I'm just curious because I made one to see why they aren't well respected, I would say it turned out pretty good. Tried making a typical one (one that uses TCP) but I had no way to test it over WAN.

Github UN (if you're interested in source)- Lukeres.

Link:<http://github.com/Lukeres/VC-RAT-FTP-Based-Remote-Access-Tool>

Also, happy holidays, if you celebrate them.

sh4moon - December 22, 2018, 8:09 pm

(Dec 22, 2018 09:02 PM)TerminallyIII Wrote: [\[CITE\]](#) Looking at some posts here I noticed that people don't really consider FTP RATs a thing. Has a RAT that uses FTP as a C&C server ever existed? I'm just curious because I made one to see why they aren't well respected, I would say it turned out pretty good. Tried making a typical one (one that uses TCP) but I had no way to test it over WAN.

Github UN (if you're interested in source)- Lukeres.

Link:<http://github.com/Lukeres/VC-RAT-FTP-Based-Remote-Access-Tool>

Also, happy holidays, if you celebrate them.

I would say it's because FTP isn't encrypted. You can easily see the traffic. Besides that, FTP isn't always allowed. Some firewalls (most likely corporate) will block FTP. You could try using SFTP instead. It's just FTP that's encrypted.

Angelis - December 22, 2018, 8:17 pm

(Dec 22, 2018 09:02 PM)TerminallyIII Wrote: [\[CITE\]](#) Looking at some posts here I noticed that people don't really consider FTP RATs a thing. Has a RAT that uses FTP as a C&C server ever existed? I'm just curious because I made one to see why they aren't well respected, I would say it turned out pretty good. Tried making a typical one (one that uses TCP) but I had no way to test it over WAN.

Github UN (if you're interested in source)- Lukeres.

Link:<http://github.com/Lukeres/VC-RAT-FTP-Based-Remote-Access-Tool>

Also, happy holidays, if you celebrate them.

FTP Protocol simply does not offer the flexibility other protocols do...

TerminallyIII - December 22, 2018, 8:17 pm

(Dec 22, 2018 09:09 PM)sh4moon Wrote: [\[CITE\]](#) I would say it's because FTP isn't encrypted. You can easily see the traffic. Besides that, FTP isn't always allowed. Some firewalls (most likely corporate) will block FTP. You could try using SFTP instead. It's just FTP that's encrypted. Oh, that's makes sense. I will look into that,thanks.

(Dec 22, 2018 09:17 PM)Angelis Wrote: [\[CITE\]](#) FTP Protocol simply does not offer the flexibility other protocols do...

OK I see. Thanks for the answer.

Vanilla - December 22, 2018, 8:20 pm

Consider creating a connection string so that when setting up RAT, they do not have to modify a bunch of lines.

sh4moon - December 22, 2018, 8:25 pm

(Dec 22, 2018 09:17 PM)TerminallyIll Wrote: [\[CITE\]](#) Oh, that's makes sense. I will look into that,thanks.

OK I see. Thanks for the answer.

Try out different transports. Maybe you could use stegonography to hide the data in pictures over FTP or something.

Angelis - December 22, 2018, 8:28 pm

(Dec 22, 2018 09:25 PM)sh4moon Wrote: [\[CITE\]](#) Try out different transports. Maybe you could use stegonography to hide the data in pictures over FTP or something.

I mean over the years I have seen some interesting attempts, even using twitter as a communications platform, but really it boils down to an encrypted connection to the C&C to establish the proper needs we want now a days with Remote tools.

CyberStrike - December 22, 2018, 8:33 pm

Link : <https://github.com/Lukeres/VC-RAT-FTP-Based-Remote-Access-Tool>

Hardcoded credentials ouch, beyond that I think it's still a great contribution.

Angelis - December 22, 2018, 10:22 pm

(Dec 22, 2018 09:33 PM)SilentWatch Wrote: [\[CITE\]](#) Link :

<https://github.com/Lukeres/VC-RAT-FTP-Based-Remote-Access-Tool>

Hardcoded credentials ouch, beyond that I think it's still a great contribution.

Man, you need extremely special circumstances to use this kinda round about method.

ON THIS NOTE

I reviewed your threads and posts, you seem to talk absolute shit to gain post count without offering true advice.

Prove me wrong.

CyberStrike - December 22, 2018, 10:53 pm

(Dec 22, 2018 11:22 PM)Angelis Wrote: [\[CITE\]](#) Man, you need extremely special circumstances to use this kinda round about method.

ON THIS NOTE

I reviewed your threads and posts,
Prove me wrong.

So you like hardcoded credentials?

Angelis - December 22, 2018, 11:24 pm

(Dec 22, 2018 11:53 PM)SilentWatch Wrote: [\[CITE\]](#) So you like hardcoded credentials?
So you like talking out of your ass?

Explain yourself or silence..... ? ? ?

CyberStrike - December 22, 2018, 11:54 pm

(Dec 23, 2018 12:24 AM)Angelis Wrote: [\[CITE\]](#) So you like talking out of your ass?

Explain yourself or silence..... ? ? ?

Did you look at the source? I'm guessing not.. or you just think payloads deserve no OPSEC and burning C2's and your infrastructure is common place.

Code class RemoteControl:

```
def connectToServer(self):
```

```
session=ftplib.FTP('files.ftpserver.com','yourftpsite','yourftppassword')
```

Edit: What prevents someone now from finding your FTP server then using your password to gather info and proceed to copy then remove any and or all files? That to me sounds like an gold mine of intelligence, but of course OPSEC is not a consideration.

Edit to the Edit: Because I don't know about your coding abilities I'll help you by posting a link

<https://docs.python.org/2/library/ftplib.html>

And yes I am quite sure that you will rant and rave tell me how I use google to figure things out but some people need links such as yourself, who couldn't denote hard coded creds will be used. Or denote the difference between Java and Javascript and what PowerShell processes and executes.

(Dec 18, 2018 06:16 PM)Angelis Wrote: [\[CITE\]](#) Can confirm this method works.

Java is not executed the same method as executable's in Windows environments. Thus bypassing many existing security checks.

Nice write up OP. Thanks for sharing.

I really don't like to be rude, so I haven't gone down that road.

Angelis - December 23, 2018, 6:23 am

(Dec 23, 2018 12:54 AM)SilentWatch Wrote: [\[CITE\]](#) Did you look at the source? I'm guessing not.. or you just think payloads deserve no OPSEC and burning C2's and your infrastructure is common place.

Code class RemoteControl:

```
def connectToServer(self):
```

```
session=ftplib.FTP('files.ftpserver.com','yourftpsite','yourftppassword')
```

Edit: What prevents someone now from finding your FTP server then using your password to gather info and proceed to copy then remove any and or all files? That to me sounds like an gold mine of intelligence, but of course OPSEC is not a consideration.

Edit to the Edit: Because I don't know about your coding abilities I'll help you by posting a link

<https://docs.python.org/2/library/ftplib.html>

And yes I am quite sure that you will rant and rave tell me how I use google to figure things out but some people need links such as yourself, who couldn't denote hard coded creds will be used. Or denote the difference between Java and Javascript and what PowerShell processes and executes.

I really don't like to be rude, so I haven't gone down that road.
I can tell your going to annoy me around here.

CyberStrike - December 23, 2018, 9:08 am

(Dec 23, 2018 07:23 AM)Angelis Wrote: [\[CITE\]](#) I can tell your going to annoy me around here.
Great there is an ignore option, use it.

Edit: Best of luck to you mate

I.M.P - December 23, 2018, 9:09 am

(Dec 23, 2018 07:23 AM)Angelis Wrote: [\[CITE\]](#) I can tell your going to annoy me around here.
I can tell your just another ass around the block ?

Angelis - December 23, 2018, 9:34 am

(Dec 23, 2018 10:09 AM)Code_T1m3 Wrote: [\[CITE\]](#) I can tell your just another ass around the block ?
Wait until you get to know me ;-)

Viotto01 - December 24, 2018, 4:37 am

(Dec 22, 2018 09:09 PM)sh4moon Wrote: [\[CITE\]](#) I would say it's because FTP isn't encrypted. You can easily see the traffic. Besides that, FTP isn't always allowed. Some firewalls (most likely corporate) will block FTP. You could try using SFTP instead. It's just FTP that's encrypted.
Also TCP isn't encrypted actually,
but you can implement a custom data encryption as many software (including #) do.
I don't see the point on why you should use the FTP protocol over TCP for programs which need to transfer any kind of data (and not just files).

Nick (Name) - December 24, 2018, 4:55 am

(Dec 24, 2018 05:37 AM)Viotto01 Wrote: [\[CITE\]](#) Also TCP isn't encrypted actually,
but you can implement a custom data encryption as many software (including #) do.
I mean what is TLS supposed to be then?

Vuln - December 24, 2018, 5:06 am

(Dec 24, 2018 05:55 AM)Nick (Name) Wrote: [\[CITE\]](#) I mean what is TLS supposed to be then?
TLS is above the transport layer, it is hardly different from "manual" encryption, although obviously depending on the implementation.

Viotto01 - December 24, 2018, 5:10 am

(Dec 24, 2018 05:55 AM)Nick (Name) Wrote: [\[CITE\]](#) I mean what is TLS supposed to be then?
A method for channel-level encryption which can be used in this case, as well.
What I meant was, that we can encrypt data in custom ways even through an unencrypted channel such as TCP or FTP.
So I don't get the point on why a RAT application should be based on FTP instead of TCP.