

Forum:[Hack Forums](#)

Thread: [Antivirus Detects Shell](#)

iPwnage - September 30, 2010, 11:42 am

Hey,

I have been trying to upload different shells to a site through cpanel. The problem is that the antivirus immediately detects the file as a shell and deletes it (unfortunately). I have tried with encrypted shells but still no luck. Opening remote urls is also disabled. Any ideas?

nigganigganigga - September 30, 2010, 12:19 pm

(Sep 30, 2010 11:42 AM)iPwnage Wrote: [\[CITE\]](#) Hey,

I have been trying to upload different shells to a site through cpanel. The problem is that the antivirus immediately detects the file as a shell and deletes it (unfortunately). I have tried with encrypted shells but still no luck. Opening remote urls is also disabled. Any ideas?

Are you talking about PC's antivirus or cPanel 'antivirus'?

Tate - September 30, 2010, 12:20 pm

(Sep 30, 2010 12:19 PM)MarkuzZ Wrote: [\[CITE\]](#) Are you talking about PC's antivirus or cPanel 'antivirus'?

That's what I'd like to know. If it's just your PC antivirus, don't save the shell.php, just click on 'New File', rename it to 'Shell.php', then paste the shell php source into 'Shell.php'.

I don't know much about cPanel Antiviruses, I didn't even know they existed.

@Mark, can you tell us more about those ?

nigganigganigga - September 30, 2010, 12:24 pm

(Sep 30, 2010 12:20 PM)Tate Wrote: [\[CITE\]](#) That's what I'd like to know. If it's just your PC antivirus, don't save the shell.php, just click on 'New File', rename it to 'Shell.php', then paste the shell php source into 'Shell.php'.

I don't know much about cPanel Antiviruses, I didn't even know they existed.

@Mark, can you tell us more about those ?

You can upload the shell as {shell.txt} then rename it to {shell.php}

OR

Make an external uploader in php and upload the shell.

Tell me if these 2 solutions works.

iPwnage - September 30, 2010, 12:34 pm

Hey, it is not my PC's antivirus, it is on a remote server where I have access to cpanel (with root). When I upload any shell using the uploader, I get an error saying "Virus (c99 900)" or "(PHP Shell)" detected. I have tried pasting the source into a new file, also uploading as text, it detects both. :/ Whats a good alternative uploade

(I tried another cpanel uploader, but that one didnt even give an error, it just failed to upload)

Here is a screenshot:

[img]http://img705.imageshack.us/img705/3664/infodo.png[/img]

nigganigganigga - September 30, 2010, 12:51 pm

Find a source on internet of an uploader and upload your shell.

hacc - September 30, 2010, 12:52 pm

Yeah upload an uploader php file, and then use it to upload the shell.

nigganigganigga - September 30, 2010, 12:59 pm

If you need help PM me with your teamviewer details I'll do it for you. ;)

hamza-net - September 30, 2010, 2:15 pm

convert the shell into ASCII undetectable it happned to me when i try to upload a shell through cpanel ftp i face this problem so the only solutin i think is to convert.

cale - September 30, 2010, 3:40 pm

Most webhosts have ClamAV but they dont have it monitoring. You may just try to enter a 4 line rce script to see if it detects that.

nazariy - September 30, 2010, 4:16 pm

Just encode in base64 or other.

hacc - September 30, 2010, 7:51 pm

(Sep 30, 2010 11:42 AM)iPwnage Wrote: [\[CITE\]](#) Hey,

I have been trying to upload different shells to a site through cpanel. The problem is that the antivirus immediately detects the file as a shell and deletes it (unfortunately). I have tried with encrypted shells but still no luck. Opening remote urls is also disabled. Any ideas?

(Sep 30, 2010 04:16 PM)nazariy Wrote: [\[CITE\]](#) Just encode in base64 or other.

Learn to Read lmao.

Clearly said its already encrypted.

cale - September 30, 2010, 11:06 pm

Try a simple rce script and if it doesn't work try a cgi shell.

nazariy - October 1, 2010, 7:20 am

(Sep 30, 2010 07:51 PM)hac Wrote: [\[CITE\]](#) (Sep 30, 2010 04:16 PM)nazariy Wrote: [\[CITE\]](#) Just encode in base64 or other.

Learn to Read lmao.

Clearly said its already encrypted.Encoding just once may be not enough.
And it's signature gets recognized.

Encode Unique Shells Multiple times.

Or Just use a very simple shell.

Idiot.

iPwnage - October 1, 2010, 9:40 am

Hey, after uploading a couple of shells yesterday, the servers were shutdown. (:P) So I will have to wait until they come back up until I can test with more shells. Thanks for all the useful replies :)

Could you please explain a bit more about CGI shells? Some of the sites have a CGI directory, but the tutorials that I saw about CGI shells seem to need to use a perl script (which I cannot execute since I don't have access to a shell or SSH [i get closed off as soon as i login]).

If the above paragraph is completely N00BY I apologize, since I have only worked with PHP shells until now, and I have never actually come across CGI shells.

nazariy - October 1, 2010, 11:17 am

(Oct 1, 2010 09:40 AM)iPwnage Wrote: [\[CITE\]](#) Hey, after uploading a couple of shells yesterday, the servers were shutdown. (:P) So I will have to wait until they come back up until I can test with more shells. Thanks for all the useful replies :)

Could you please explain a bit more about CGI shells? Some of the sites have a CGI directory, but the tutorials that I saw about CGI shells seem to need to use a perl script (which I cannot execute since I don't have access to a shell or SSH [i get closed off as soon as i login]).

If the above paragraph is completely N00BY I apologize, since I have only worked with PHP shells until now, and I have never actually come across CGI shells.

Yes,

Search for CGI-telnet.

Coded in perl.

Upload to server and change the CHMOD to 755

You would access it like a normal shell.

You will have the ability to Upload/Download/Execute Commands on the server.

Blazin - May 25, 2015, 6:39 pm

Most antiviruses these days detect shells.

EG : AVG, etc. Depending on what kind of antivirus they have CLAMAV, etc.

hahdbwoannniabs - May 25, 2015, 8:04 pm

(May 25, 2015 06:39 PM)Blazin Wrote: [\[CITE\]](#) Most antiviruses these days detect shells.

EG : AVG, etc. Depending on what kind of antivirus they have CLAMAV, etc.

1. Look at the date the thread was created
2. Realize you're fucking retarded
3. Give me a -3 for insulting you, I already know you're going to