Hexing Your C99 to Graphics Interchange Format

By: Warpboy

Amazingly, alot of people just get there hands on the c99.gif not knowing how it was made. This tutorial will cover how to convert your php backdoors (c99 is used as an example in this tutorial) to graphics interchange format (gif), manually. It's very easy, if your quick and know a little about hexing, you should be done in a matter of minutes.

What do you need?

c99 in php format (or another php backdoor in php format)
Hex editor (hex probe is used in this tutorial -- download here: http://www.hexprobe.com/)
A cerebral cortex, that is halfway working.

Let's get started, open up your c99.php in the hex editor, see figure F1 below.

F1

Once you have the file opened, you will see the file in hex.Your offset location should be: 0000000000. See figure F2 below.

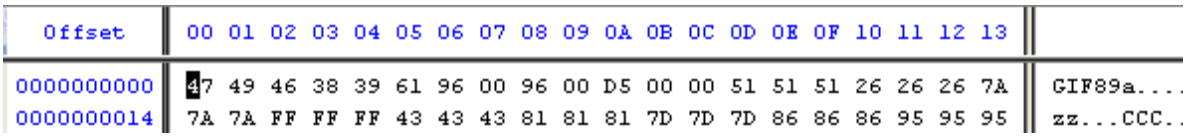
Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
0000000000	3C 3F 70 68 70 0D 0A 2F 2F 53 74 61 72 74 69 6E 67 20 63 61 6C 6C 73 0D
0000000018	0A 69 66 20 28 21 66 75 6E 63 74 69 6F 6E 5F 65 78 69 73 74 73 28 22 67
0000000030	65 74 6D 69 63 72 6F 74 69 6D 65 22 29 29 20 7B 66 75 6E 63 74 69 6F 6E
0000000048	20 67 65 74 6D 69 63 72 6F 74 69 6D 65 28 29 20 7B 6C 69 73 74 28 24 75
0000000060	73 65 63 2C 20 24 73 65 63 29 20 3D 20 65 78 70 6C 6F 64 65 28 22 20 22
0000000078	2C 20 6D 69 63 72 6F 74 69 6D 65 28 29 29 3B 20 72 65 74 75 72 6E 20 28

F2

If your using hexprobe as you highlight the offsets (left column) the hex values decrypted (into ASCII) in the right hand column highlights. Each offset has a value, in this case 3C 3F 70 68 70 stand for "<?php" in the file.

Moving on, lets go ahead and open up a gif image in the hex editor and see what it looks like. See figure F3.

Tip: You can open more than 1 file in hexprobe, making it easy to jump back in forth between the two, which we will be doing.

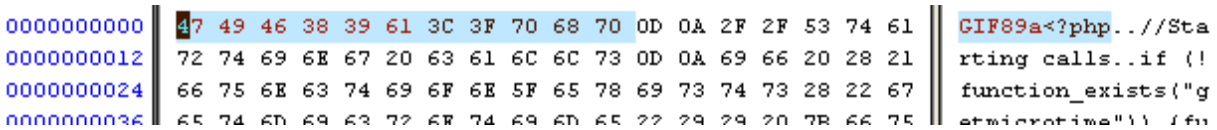


Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13	
0000000000	47 49 46 38 39 61 96 00 96 00 D5 00 00 51 51 51 26 26 26 7A	GIF89a....
0000000014	7A 7A FF FF FF 43 43 43 81 81 81 7D 7D 7D 86 86 86 95 95 95	zz...CCC..

F3

See the GIF89a? Unless your blind or have bad eye sight you should. What is GIF89a? GIF refers to a graphics file in an image format according to Graphics Interchange Format. and the 89a refers to the version of the image file, Version 89a (July, 1989). In hex GIF89a is: 47 49 46 38 39 61 96.

Now how do we make our php file be read as a gif file? Easy, since GIF89a makes browsers read the gif file as a gif file. We forge our php file into making it look like a gif file. All you have to do is copy the hex values 47 49 46 38 39 61 96 from the gif file, and paste them directly in front of the 3C 3F 70 blah blah on the offset 0000000000. Your c99.php file should look like figure F4 below.



0000000000	47 49 46 38 39 61 3C 3F 70 68 70 0D 0A 2F 2F 53 74 61	GIF89a<?php..//Sta
0000000012	72 74 69 6E 67 20 63 61 6C 6C 73 0D 0A 69 66 20 28 21	rting calls..if (!
0000000024	66 75 6E 63 74 69 6F 6E 5F 65 78 69 73 74 73 28 22 67	function_exists("g
0000000036	65 74 6D 69 63 72 6F 74 69 6D 65 22 29 29 20 7B 66 75	etmicrotime")) {fu

F4

Now just click save as, and save c99.php as c99.gif. Then go to the directory you saved it in. View the file, nothing should be displayed. c99.gif is mostly used in remote file inclusions. Thats pretty much the end of this tutorial. I hope you learned something.

Warpboy
www.securitydb.org
Joln Today ^^