A Closer look on C&C Panels

Seminar on Practical Security
Tandhy Simanjuntak

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

- Machine to manage bot
- Send instructions and receive data

C&C Servers
Introduction

How It Works

Infect the system

Gather credentials - PII

Upload data to C&C Server
Detection Methods

Detection Methods

Google Dorks
Network Traffic Analysis
Public C&C Trackers
Detection Methods

Google Dorks

Google Advance search techniques
i.e. inurl, intitle, filetype, etc.

Network Traffic Analysis

Public C&C Trackers
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

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=q0Han12ck5warpvNtz1TCRkTBN1K6h0RwwAJLzACqgsmAC1MYTORBCigASvQNEiKFrdfRBIm0EvoUmCvNEIpIF
KsVgduLkqGskx5sm2Bste0VgoCiu9wa0FmcvBncvNEI0Z2bz9mcj1WtoACM3DMI2EiVJHzhVXugEUSElKvO Pi
p1Gz8psqV4kkg2dDegcD1zd3bkSwaxPmWnwMwj1NoMmz4Azmgz72yW0vYKhjYOmWnkJWZmRmHydM1l7oHTP/
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

==AfQMFBRVkuIRFIOICM0jmx0DdkRnlL52b0NXYu9mag8ULgMzMzj0vZmbp5ipBFgajv2ZvRmlX0Wd0Fmc0N3LV
0DcjR3kTtvHdHJHdzBybtACdvlncjNHiHliKgQyVxmb39GZ/
I2bsj3Lw8SMfN0Nh1Tw58yc1Twxam95MvKpGch9Gc055Zn9Y64Hd0HGl0JXY0NnlYvmbp1GfQMXZ5By7tACNZ2TMgl
XlG0uhc5h5ZU9gdfMvbp1g11CI5MzH0T7vBNMyLryG0ZFMonXy55Zn9Gzu0Wd0Fmc0N3LvoDcjR3kTvHdHJHzdBy
btACdvlncjNHiHli1KgQyVxmb39GZ/
I2bsj3Lw8SMfN0HuOzUSZ2Bvctxwam95MvKpGch9Gc055Zn9Y64Hd0HGl0JXY0NnlS3ZuIXZu1Wbi
```
Independent researchers

- Zeus Tracker - https://zeustracker.abuse.ch/
- SpyEye Tracker - https://spyeyetracker.abuse.ch/
- Palevo Tracker - https://palevotracker.abuse.ch/
- Feodo Tracker - https://feodotracker.abuse.ch/
Detection Methods
Securing C&C Panels

https://pixabay.com/get/5295f3a7172794c94c16/1439055210/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
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

- Encryption and authentication
- RC4 algorithm
- Hard-coded in configuration file
- Zeus and Citadel

Extracted from configuration file:

```php
$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:
Compromise methods
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

- Apache treats .php as a valid .php \(\rightarrow\) file.php.
Compromised Methods

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

- Find others’ vulnerabilities
- Upload remote management shells
- Notorious Datacenter support systems – Pwning through outer sphere: Exploitation Analysis of Help Desk Systems

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

<table>
<thead>
<tr>
<th>Insecure Deployment</th>
<th>Exposed Directory Structure</th>
<th>Unprotected Components</th>
<th>SQL Injection, XSS</th>
<th>Open Ports</th>
<th>Weak Password and Login Page Key</th>
</tr>
</thead>
</table>

**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](https://www.apachefriends.org/faq_linux.html)
Compromised Methods

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

Index of /info

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

Apache Server at pu[...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 WAF Server at ohan.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. 
```

Index of /img/web/redirect
Compromised Methods

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

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

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

- Parent Directory
- tf_772bec_6b2b9bc7.php.inc

Protected by [AF Server at].com Port 80
Compromised Methods

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#8226</td>
<td>Connecting to MySQL as &lt;b&gt;'sayno2ga_foxpp'&lt;/b&gt;</td>
</tr>
<tr>
<td>#8226</td>
<td>Selecting DB &lt;b&gt;'sayno2ga_foxpp'&lt;/b&gt;</td>
</tr>
<tr>
<td>#8226</td>
<td>Updating table &lt;b&gt;'botnet_list'&lt;/b&gt;</td>
</tr>
<tr>
<td>#8226</td>
<td>Creating table &lt;b&gt;'botnet_reports'&lt;/b&gt;</td>
</tr>
<tr>
<td>#8226</td>
<td>Updating table &lt;b&gt;'botnet_reports_140601'&lt;/b&gt;</td>
</tr>
<tr>
<td>#8226</td>
<td>[1] Updating table &lt;b&gt;'botnet_webinjects_group'&lt;/b&gt;</td>
</tr>
</tbody>
</table>
```

---

TRUNCATED
Compromised Methods

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

Citadel C&C Panel:

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

```
Compromised Methods

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

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


