

Corporate Espionage FOR DUMMIES

The Hidden Threat of
Embedded Web Servers

Michael Sutton
VP, Security Research



whois

Company

- Browser/email security
- VP, Security Research

Background

- Founding Member – Cloud Security Alliance
- SPI Dynamics – acquired by HP
- iDefense – acquired by VeriSign

Research

- Web security
- Client-side vulnerabilities



Agenda



Agenda



What does it mean to be in a hyperconnected world?



What has an IP address in your home?



Television



DVR



Blu-ray/DVD



Webcam



Large Appliances



Video Game Console



Kitchen Appliances



Phone



What has an IP address in your office?



Printer



Scanner



Networking



Security System



HVAC



NAS



Video Conferencing



Photocopier



EWS Definition

What is an Embedded Web Server? There's no universally accepted definition, but for our purposes, we'll require the following:

1. Web server installed on the hardware during the manufacturing process (not an optional component)
2. Not designed for high performance
3. Limited functionality
4. Serves as an administrative interface to the host hardware



Public Service Announcement



Threats

Overall

- DoS – Disable functionality
- Privacy – Access confidential data
- Data Integrity – Alter confidential data
- Financial – Unauthorized use of bandwidth and services
- Compromise – Firmware upgraded with new functionality

External

- Improperly configured networks can make internal appliances Internet accessible
- Vendors target *ease of use* and EWSs therefore have functionality enabled *out of the box* with a default password or are wide open

Internal

- Devices with EWS generally not considered during security audits and are not therefore monitored/segregated
- Insiders have the advantage of physical access to the devices



Java Vulnerabilities?

Attacks?

1. Change the preset coffee settings (make weak or strong coffee)
2. Change the amount of water per cup (say 300ml for a short black) and make a puddle
3. Break it by engineering settings that are not compatible (and making it require a service)

JUNE 17, 2008 12:04 PM PDT

Internet-connected coffee maker has security holes

by Elinor Mills

Print E-mail

14 comments

Tweet

1

Recommend

Share

An Australian man has discovered security vulnerabilities in his Internet-connected coffee maker that could allow a remote attacker to not only take over his Windows XP-based PC but also make his coffee too weak.

Craig Wright, a risk advisory services manager at professional services firm BDO, found several security holes, including a buffer overflow in the Internet Connection software that links his Jura F90 coffee maker to his PC.

Once connected to the Internet, the high-end coffee maker, which retails for nearly US\$2,000 on Amazon, lets you do things like set the strength of your coffee and get remote diagnostic help over the Internet without having to send the appliance in for service.

Wright posted the information on the vulnerabilities, and the fact that there is no patch available yet, to the BugTraQ security e-mail list on Tuesday.

A U.S.-based public relations representative for the coffee maker said she would try to reach spokespeople in the Switzerland headquarters for comment.

The threat hasn't kept Wright awake at night, although the coffee does, he said in an interview with CNET News.com at 2:30 Wednesday morning Sydney time.

"I don't know if many people would target this particular vulnerability because there probably are not a lot of coffee makers at the moment that are Internet-connected, and in my case it's behind a firewall," he said.



This \$2,000 Jura F90 coffee maker can be connected to the Internet for remote control of the settings. But it also can open up your PC to remote attacks, a security expert says.

(Credit: Jura)

However, Internet-connected appliances are the wave of the future. There is already an **Internet-connected refrigerator**, at least **one prototype of a Web-enabled oven**, and **pilot tests for dryers and water heaters**.



Energy Savings

Internet-Connected Appliances Could Lower Energy Bills

A pilot test in Washington and Oregon lets dryers and water heaters check electricity prices and decide if it's worth waiting until off-peak times.

By [Keyla Kirton InformationWeek](#)
May 15, 2006 12:00 AM

Jerry Brous' clothes dryer drives a hard bargain. Every five minutes, it checks the current electricity price over the Internet. If the price is above the threshold Brous set, the dryer doesn't run. Save the clothes for later--and don't get soaked.

Brous is one of 200 people in Washington and Oregon taking part in an experiment that uses real-time pricing data to let people make smarter choices about energy use. It's a tiny project with the potential to significantly change electricity markets at a time when energy is back on top of public policy concerns.



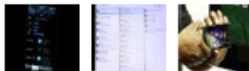
More Insights

White Papers

- [How to Effectively Measure and Monitor Activity in Your Portal Environment](#)
- [Going Into School Teaching After Academic Study](#)

Videos

Sponsored by:



Dryers and Water Heaters

The GridWise Initiative, led by the Pacific Northwest National Laboratory, is testing dryers, thermostats, and water heaters that are wirelessly connected to a server, which uses a broadband connection to fetch prices. Homeowners also can set monthly energy budgets and monitor in real time whether they're sticking to them. In another experiment, 150 dryers are equipped with a chip that will respond to instability on the power grid and shut off the heating units on the dryers for a few minutes. Spread across millions of homes, this program could provide a shock absorber in the grid, giving producers the few minutes needed at times of peak demand to bring new power online.

The project takes a market approach to trying to lower power consumption--or shift it to off-peak times. That could let utilities put off building new power plants, says Don Hammerstrom, Pacific Northwest National Lab's project manager.

- Energy savings and home automation will continue to drive *Internet enabled* devices
- Currently serves as a differentiator for high end appliances
- Combination of EWSs, HTTP(S) aware client side applications



Strange Sightings - Projectors



KEC-1003PJB

HP Digital Projector xp8020

Home

Projector

Networking

Management

Device Info

Select Language

Other Links

[Help](#)

[Support](#)

[HP Home](#)

Device Info



Status:	Standby
Current lamp hours:	1242
System Contact:	Albert Berglund
Support Phone Number:	541.737.6428
System Location:	Kelley Engineering Center 1003

Firmware Version:	5.0 - 2.1
Wired IP Address:	128.193.38.152
Wireless IP Address:	[Unknown]
Serial Number:	??????????????
Admin Password:	[Set]

HTTP/1.1 200 OK
Server: **microChai ver 2.0**
Cache-Control: no-cache
Expires: Mon, 24 Nov 2003
00:00:00 GMT
Connection: Keep-Alive
Transfer-Encoding: chunked



Strange Sightings - Projectors



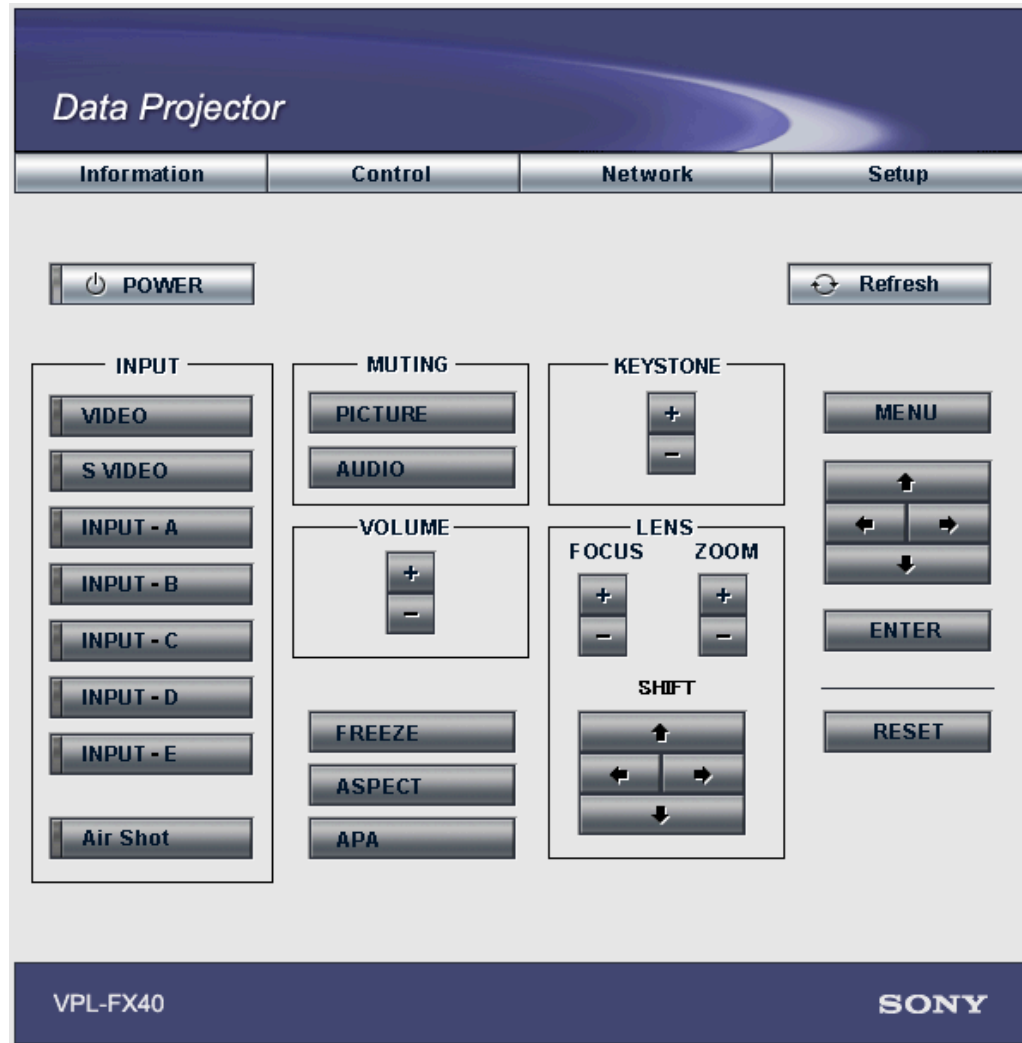
Office Prank

Step 1 – Scan the network for web servers with the following header:

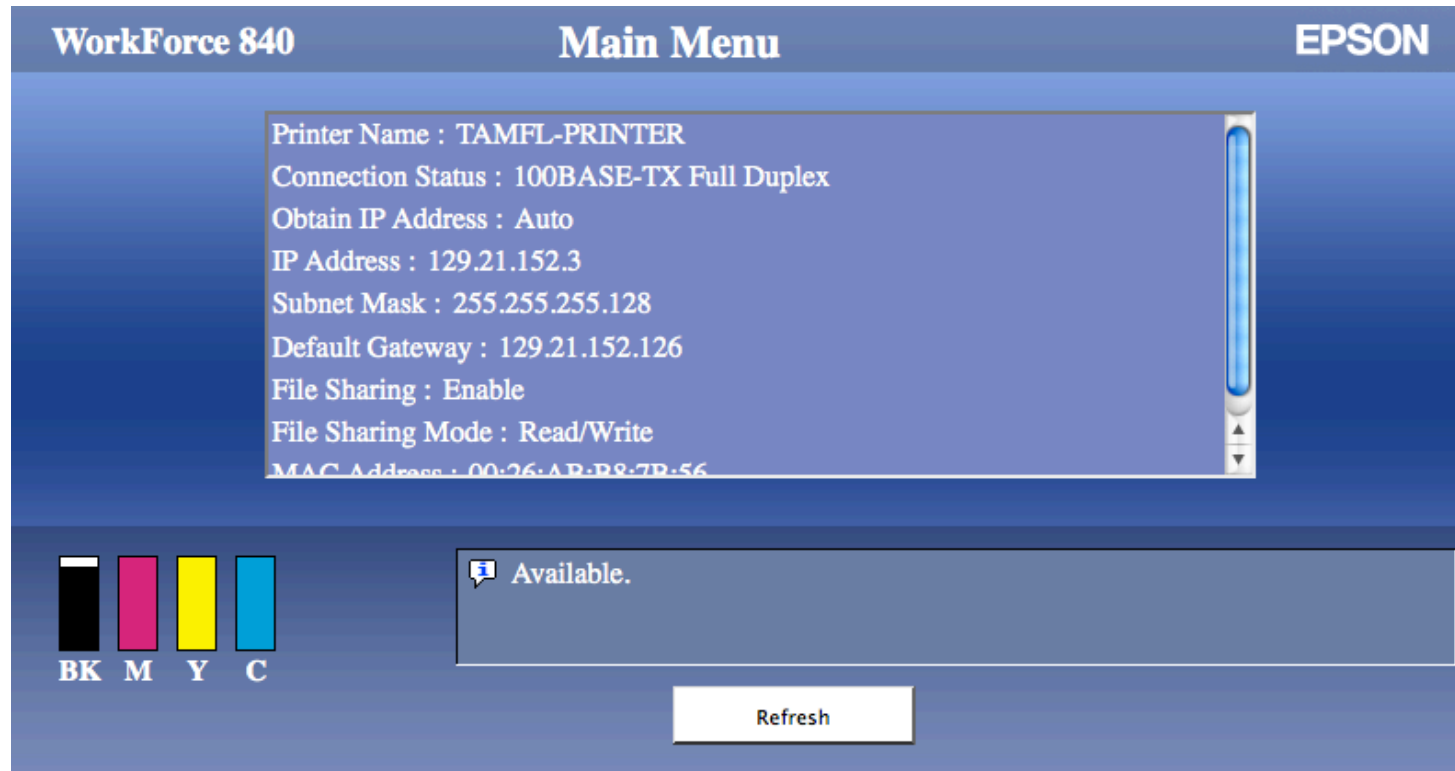
Server: Network Projector

Step 2 – Wait for the meeting to start

Step 3 – Continually adjust focus. When presenter attempts to fix, power off.



Strange Sightings - Printers



The screenshot shows the 'Main Menu' for an Epson WorkForce 840 printer. The interface is blue and white. At the top, it says 'WorkForce 840', 'Main Menu', and 'EPSON'. The main content area displays the following information:

- Printer Name : TAMFL-PRINTER
- Connection Status : 100BASE-TX Full Duplex
- Obtain IP Address : Auto
- IP Address : 129.21.152.3
- Subnet Mask : 255.255.255.128
- Default Gateway : 129.21.152.126
- File Sharing : Enable
- File Sharing Mode : Read/Write
- MAC Address : 00:26:AB:B8:7D:56

Below the settings is a status bar with four ink level indicators: BK (Black), M (Magenta), Y (Yellow), and C (Cyan). To the right of the indicators is a message box that says 'Available.' and a 'Refresh' button.





If you're too lazy to walk over to the printer to check the ink cartridges...
...you're also too lazy to walk to the store to replace them!



Remember

Strange Sightings - Kiosks

famous footwear 





MAKE TODAY CAREFREE

welcome!

Are you ready to search over
a million pairs of shoes?

How would you like to search?

-  I have the right shoes in my hand, but I'm looking for a **different size or color**
-  I want to search by **brand**
-  I want to search by **style**

Please swipe your Badge 

UCLA General Services

© 2011 UCLA General Services. All Rights Reserved.



Process

Goal

- Fingerprint at least 1M web servers and identify as many EWSs as possible to better understand the threat that they may pose

Challenges

- Millions of IP addresses need to be scanned
- Scanning must therefore be very light weight and scalable
- Existing fingerprinting tools (i.e. NMAP) do not have a strong database of EWS data

Options

- Traditional scanning/fingerprinting tools
- GHDB (Google Hacking Database)
- Header fingerprinting scans



Nmap

Canon imageRUNNER C2880 Photocopier

Nmap Results

```
$ sudo nmap -O 131.96.246.162
```

```
[snip]
```

```
Aggressive OS guesses: Apple AirPort Express WAP v6.3 (92%), AirSpan  
ProST WiMAX access point (91%), m0n0wall FreeBSD-based embedded firewall  
version 1.22 - 1.23b1 (89%), Canon imageRUNNER C5185 printer (89%),  
SonicWALL SonicOS Enhanced 5.2.0.1-21o (88%), FreeBSD 6.2-RELEASE (88%),  
VxWorks: Apple AirPort Extreme v5.7 or AirPort Express v6.3; Canon  
imageRUNNER printer (5055, C3045, C3380, or C5185); Kyocera FS-4020DN  
printer; or Xerox Phaser 8860MFP printer (87%), IBM DCS9900 NAS device  
(87%), Nokia IP650 firewall (IPSO 4.0 and CheckPoint Firewall-1/VPN-1  
software) (85%), HP LaserJet P2055dn printer (85%)  
No exact OS matches for host (test conditions non-ideal).
```

Server Headers

```
HTTP/1.1 200 OK
```

```
Date: SUN, 16 JUL 2011 19:13:57 GMT
```

```
Server: CANON HTTP Server Ver2.21
```

```
Content-Type: text/html
```

```
Transfer-Encoding: chunked
```



GHDB



To Top page

Device

Job Status

Mail Box

Direct Print

Address

Add. Func.

▶ [Mail to Administrator](#)

Remote UI



Remote UI
Copyright CANON INC. 2005
All Rights Reserved

Device Name :

iR2270

Product Name :

iR2270

Location :

NW011

Last Updated : 05/16/2011 13:15:33



● Printer Status : **Ready to print.**

● Scanner Status : **Ready to scan.**

Language :

English

System Manager :

[RadHS Support](#)

Support :



Canon

GHDB



トップページへ

デバイス

ジョブ

ボックス

アドレス

ユーザモード

▶ [管理者へメール](#)



Canon

リモートUI



リモートUI
Copyright CANON INC. 2006
All Rights Reserved

デバイス名 : iR C2570

製品名 : iR C2570

設置場所 :

最終更新 : 2011 05/17 05:15:00



- プリンタ : スリープ中です。
- スキャナ : スリープ中です。
- ファクス : ファクスできます。

表示言語の切替 :

システム管理者 :

サポートリンク :

GHDB

Web [Images](#) [Videos](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more](#) ▼



intitle:"Remote UI" "Copyright CANON INC" "Printer Status" Search

About 127 results (0.20 seconds)

[Go to Google.com](#) [Advanced search](#)

Everything

Images

Videos

News

Shopping

More

[Remote UI <Top page > : iR C3480 : iR C4080](#) 🔍

16 Apr 2011 ... **Printer Status : Printer Status** Sleep mode. ... Copyright : Remote UI
Copyright CANON INC. 2008. All Rights Reserved ...
[68.181.150.20/ - Cached](#)

[Remote UI <Top page > : iR C3480 : iR C3480](#) 🔍

14 Apr 2011 ... **Printer Status : Printer Status** Ready to print. ... Copyright : Remote UI
Copyright CANON INC. 2008. All Rights Reserved ...
[128.36.107.74/ - Cached](#)

Challenges

- Google clearly suppresses/blocks GHDB queries (Bing can actually be better)
- UI Internationalization/rebranding requires many queries for broad coverage
- API queries are throttled to a set amount per day
- Searches for potentially vulnerable systems can lead to source IP blocks, especially when queries are automated

Google Sorry...

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

See [Google Help](#) for more information.



Header Scanning

```
HTTP/1.0 200 OK
Date: SUN, 23 APR 2011 21:31:45 GMT
Server: CANON HTTP Server Ver2.21
Set-Cookie: iR=3753281; path=/
Content-Type: text/html
Transfer-Encoding: chunked
```

Approach

- Simple multi threaded Perl script to send HEAD requests
- Amazon EC2 micro instances leveraged – highly scalable, low cost

Advantages

- Highly scalable – small request/response
 - Ease of automation
 - Content based signatures not required
 - EWS header information unlikely to be spoofed
- Limitations

Challenges

- Not all EWSs have a unique Server string or header info.

Result

- Goal of fingerprinting 1M web servers achieved



Shodan

- Comprehensive, searchable database of web server headers and telnet banners
- Provides country of origin IP and rDNS data
- Commercial service – users must register to receive >10 results and pay for >50

Results 1 - 10 of about 3250 for CANON HTTP Server Ver2.21

+ Add to Directory	Export Data
» Top countries matching your search	
United States	1,700
Korea, Republic of	337
Japan	305
Canada	175
Taiwan	113

[128.36.110.2](#)

Added on 24.04.2011



Details

[yale128036110002.central.yale.edu](#)

HTTP/1.0 200 OK

Date: SUN, 24 APR 2011 05:14:57 GMT

Server: **CANON HTTP Server Ver2.21**

Set-Cookie: iR=1225169; path=/
Content-Type: text/html

Transfer-Encoding: chunked

shodanhq.com



Agenda



What could possibly go wrong?



Printers/Scanners

“Mistakes are the portals of discovery”
- James Joyce (1882-1941)



HP Printers/Scanners

Headers	LaserJet	OfficeJet	Photosmart
Server: Mrvl-R1_0	✓		
Server: \$ProjectRevision: 5.0.1.23 \$ Server: \$ProjectRevision: 4.2 \$ Server: \$ProjectRevision: 4.0.2.38 \$ Server: \$ProjectRevision: 4.7.1.12 \$	✓		
Server: HP-ChaiServer/3.0 SERVER: HP-ChaiSOE/1.0	✓		
Server: Virata-EmWeb/R6_2_1	✓	✓	✓

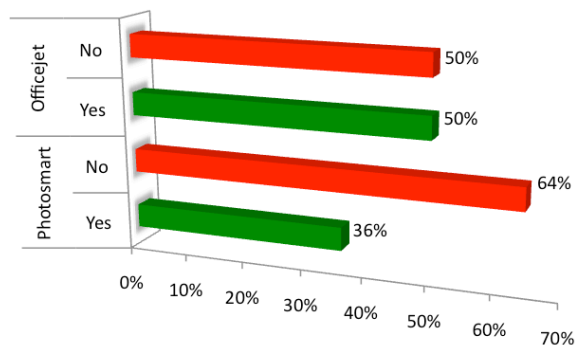
Numerous embedded web servers across hundreds of products



HP Printers/Scanners

Headers	ShodanHQ
Server: Mrvl-R1_0	22
Server: \$ProjectRevision: 5.0.1.23 \$	673
Server: \$ProjectRevision: 4.2 \$	1,498
Server: \$ProjectRevision: 4.0.2.38 \$	4,514
Server: \$ProjectRevision: 4.7.1.12 \$	946
Server: HP-ChaiServer/3.0	18,011
SERVER: HP-ChaiSOE/1.0	39,071
Server: Virata-EmWeb/R6_2_1	59,269
Total	124,004

Admin Password Set for Identified Scanners?



HP Printers/Scanners

Purpose

- Manage devices – security, logging, networking, etc.
- Monitor devices – ink levels, alerts, etc.

Observations

- Laserjet printers rarely have password protection enabled
- Hundreds of thousands of HP devices are web accessible

Risk

- Reconfigure device – networking, UI, etc.
- DoS – lock device access, cancel jobs, etc.
- **WebScan – remotely access scans and trigger new jobs**
- **Fax Forwarding – forward incoming faxes**



HP Fax Forwarding

The screenshot displays the HP Officejet Pro 8500 A909g web interface. At the top, the HP logo and model name are shown. Below this, the device status is 'Ready' and the date is 'Thursday, 2011-05-12 10:19:01'. The navigation menu includes 'Home', 'Information', 'Settings', 'Networking', and 'Bluetooth'. The 'Fax' section is expanded, showing options like 'Fax Speed-dial', 'Basic Fax Setup', 'Advanced Fax Setup', 'HP Digital Fax', 'Junk Fax Blocker', and 'Fax Options'. The 'Fax Forwarding' settings are highlighted, showing a dropdown menu set to 'On - Forward', a 'Fax Forward Number*' field containing '1-800-466-9633', and fields for 'Start Date(DD-MM-YY)', 'Start Time(HH:MM)', 'Stop Date(DD-MM-YY)', and 'Stop Time(HH:MM)'. A red circle highlights the 'Fax Forwarding' dropdown, and a red bracket groups the 'Fax Forward Number*' and date/time fields. A red text annotation on the right says 'Forward all incoming faxes to an external fax number'. The interface also includes 'Order Supplies' and 'Support' buttons, and a 'Clear Fax Logs' section at the bottom.

HP Officejet Pro 8500 A909g

HP71F0DC Status: Ready Thursday, 2011-05-12 10:19:01

Home Information Settings Networking Bluetooth

Fax

- Fax Speed-dial
- Basic Fax Setup
- Advanced Fax Setup
- HP Digital Fax
- Junk Fax Blocker
- Fax Options

E-mail - Digital Filing

- Outgoing E-mail Profile Setup
- E-mail Address Book
- E-mail Options

Scan - Digital Filing

- Network Folder Setup

Administrator Settings

- Security

Device

- Device Services
- Backup & Restore Settings
- Usage Tracking
- Alerts
- AutoSend
- Paper Handling
- Asset Tracking
- Memory Devices

Preferences

- Date & Time
- International
- Time Zone

Fax

Fax Forwarding

You can set the device to automatically redirect incoming faxes to another fax number.

Fax Forwarding:

Fax Forward Number* :

Start Date(DD-MM-YY): - -

Start Time(HH:MM): :

Stop Date(DD-MM-YY): - -

Stop Time(HH:MM): :

* Required Field

Apply Cancel

Clear Fax Logs

To clear the incoming and outgoing fax logs, click "Clear".

Clear

Forward all incoming faxes to an external fax number



HP Webscan

HP Photosmart C309a series

HPF1B962

Status: Ready Thursday, 2011-05-12 11:31:03

Information Settings Networking Bluetooth

++ --

- Overview
 - Device Information
 - Network Information
- Status
 - Usage Report
 - Log
- Applications
 - Webscan**
- EWS Settings
 - Language
 - Refresh Rate

Webscan

[Order Supplies](#) [Support](#)

Webscan lets you scan photos and documents from your device to your computer using a Web browser, even if you chose not to install the device software on your computer.

To use Webscan, load your original print side down in the right front corner of the glass, and then close the lid. After the original is loaded, select the image type and document size, and then click "Preview" or "Scan". (Clicking "Preview" initiates a scan and displays a preview of the original in the EWS. However, the image is not saved on the computer until you click "Scan".) To reset the preview window, click "Reset".

Note: You can only scan single-page documents from the scanner glass when using Webscan.

Note: Many Web browsers have settings that allow you to prevent pop-up messages from appearing while you are visiting websites. However, these settings can also prevent Webscan from functioning properly. To use Webscan, make sure the browser is set to allow pop-up messages to be displayed. For information about changing these settings, see the onscreen Help or documentation for your Web browser.

Image Type

- Color Picture
- Color Drawing
- B/W Picture
- Text

Document Size Letter

Quick Scan – Determine if doc. exists

Scan and download as JPEG

Preview

Scan **Reset**

中華民國	100年	5月	12日	上午	11時	31分	03秒
掃描人	100	5	12	11	31	03	
掃描時間	100	5	12	11	31	03	
掃描地點	100	5	12	11	31	03	
掃描狀態	100	5	12	11	31	03	
掃描結果	100	5	12	11	31	03	
掃描文件	100	5	12	11	31	03	
掃描格式	100	5	12	11	31	03	
掃描大小	100	5	12	11	31	03	
掃描速度	100	5	12	11	31	03	
掃描品質	100	5	12	11	31	03	
掃描解析度	100	5	12	11	31	03	
掃描顏色	100	5	12	11	31	03	
掃描模式	100	5	12	11	31	03	
掃描類型	100	5	12	11	31	03	
掃描用途	100	5	12	11	31	03	
掃描說明	100	5	12	11	31	03	

HP Webscan

What we found...

APPLICATION TO HOST A TOURNAMENT OR GAMES

Please Type or Print Clearly - Do Not Staple

Name of Tournament or Games: [REDACTED] Website URL: [REDACTED]
 Type of Tournament: Select Recreational Select & Rec

Hosting Organization: [REDACTED] Title: Treasurer Phone: [REDACTED] W
 Designate Official of Hosting Organization: [REDACTED] Phone: [REDACTED] H
 Address: PO Box 212 Email: [REDACTED] Phone: [REDACTED] FAX
 City: [REDACTED] State: NJ Zip Code: [REDACTED]

Location of Tournament or Games: [REDACTED] TEAM ENTRY DEADLINE: [REDACTED]
 Date(s) of Tournament or Games: [REDACTED] Estimated # of Teams: [REDACTED]
 Tournament or Games Director or Contact Person: [REDACTED] Phone: [REDACTED] W
 Address: [REDACTED] Email: [REDACTED] Phone: [REDACTED] H
 City: [REDACTED] State: [REDACTED] Zip Code: [REDACTED] Phone: [REDACTED] FAX

Age Groups Accepted	Types(s) of Team Accepted	B	G	Roster Size	# Guest Players Allowed	Length of Games	# Players on Field	Awards	Minimum # of Games	Entry Fee	Bond
U- 7- 8/11 2002	CE	x	x	14	4	30 min	8	Participation	3	200	-
U- 8 8/11 2001	CE	x	x	14	4	40 min	8	Participation	3	200	-
U- 9 8/11 2000	CE	x	x	14	4	40 min	8	Participation	3	200	-
U- 10 8/11 1999	CE	x	x	14	4	40min	8	Participation	3	200	-
U- 11 8/11 1998	CE	x	x	18	4	50 min	11	Participation	3	200	-
U- 12 8/11 1997	CE	x	x	18	4	50 min	11	Participation	3	200	-
U- 7 8/11 2002	FGH	x	x	14	4	30 min	8	Participation	3	200	-
U- 8 8/11 2001	FGH	x	x	14	4	40 min	8	Participation	3	250	-
U- 9 8/11 2002	FGH	x	x	14	4	40 min	8	Participation	3	250	-
U- 10 8/11 1999	FGH	x	x	14	4	40min	8	Participation	3	250	-
U- 11 8/11 1998	FGH	x	x	18	4	50 min	11	Participation	3	275	-
U- 12 8/11 1997	FGH	x	x	18	4	50 min	11	Participation	3	275	-

*List of types of teams and tournaments is on reverse side of this form.

RT RESTRICTED TOURNAMENT -Open only to members of US Youth Soccer and its State Associations.
 International Teams as listed.

UT UNRESTRICTED TOURNAMENT Other US Soccer Members Listed: Any USYSA team, US Club Soccer, Travel and Recreational Teams

The Hosting Organization agrees to be bound by and comply with the terms contained in the TOURNAMENT AND GAMES HOSTING AGREEMENT and all applicable rules of the approving State Association or Affiliate.

Signature of Designated Official of Hosting Organization: [REDACTED] Date: 12/18/09

By: [REDACTED] Title: [REDACTED]
 Date: DEC 23 2009

APPROVAL (For Official Use Only) [REDACTED]
 STATE NJYS OFFICE
 DEC 21 2009
 [REDACTED]

Signed documents



HP Webscan

What we found...

1

STATE

REPUBLICAN

STATE

GOVERNOR Vote for One	BILL CHANGERS Retail/Salesperson	Republican	7
	KEN MILLER Party, Manufacturing Executive	Republican	8
	DOUGLAS R. HUGHES Retail District Center	Republican	9
	LAWRENCE "LARRY" NARTELLI Accountant/Consultant	Republican	10
	ROBERT G. NEWMAN II Psychologist/Partner	Republican	11
	DAVID FULLY-SMITH Primary Care Physician	Republican	12
SENATOR	MIG WHITMAN Businesswoman	Republican	13
	STEVE FOKNER Businessman	Republican	14
	SAM AANESTAD Cocoa/Custodia Senator	Republican	15
LEGISLATIVE COUNCIL Vote for One	YVONNE H. GIRARD Junk/Discount	Republican	16
	BEVE DAVIS Businesswoman	Republican	17
	ABEL MALDONADO Teacher/Bus/Insurance Farmer	Republican	18
	DAVE HARRIS Businessman	Republican	19
	SCOTT L. LEVET Miner	Republican	20
SECRETARY OF STATE Vote for One	GAMON DUBIN Small Business Owner	Republican	21
	ORLY TATZ Attorney/Consultant/Businesswoman	Republican	22
CONTROLLER Vote for One	DAVID EVANS CPA/CFO	Republican	23
	TONY STRICKLAND State Senator/Businessman	Republican	24
TREASURER Vote for One	BRIAN WALTERS Businesswoman/Teacher	Republican	25

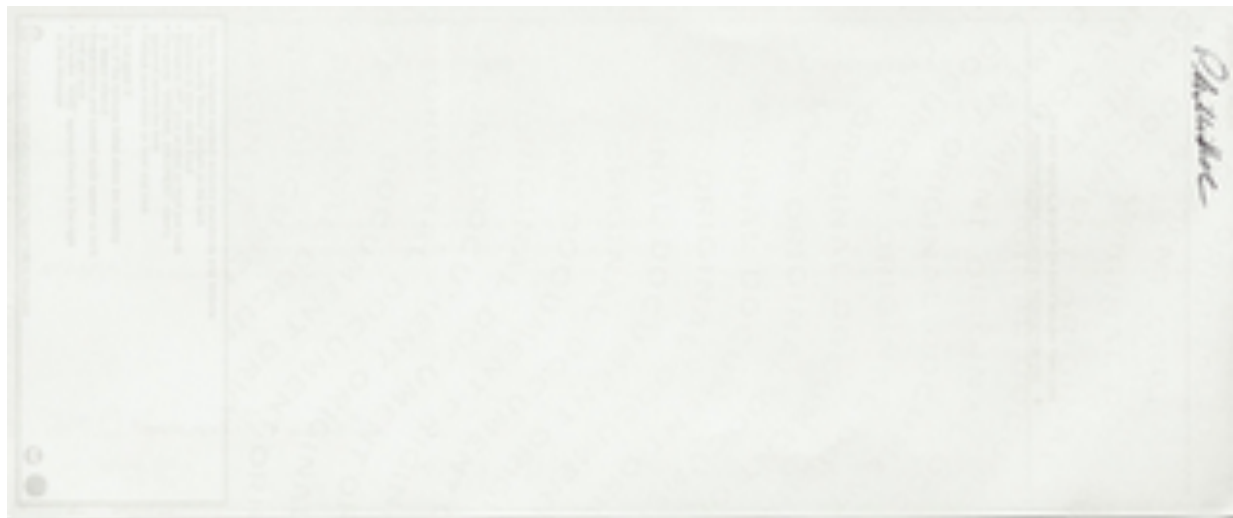
PLEASE NOTE: The order in which candidates' names appear on the ballot is determined by a coin-

Voting advice



HP Webscan

What we
found...

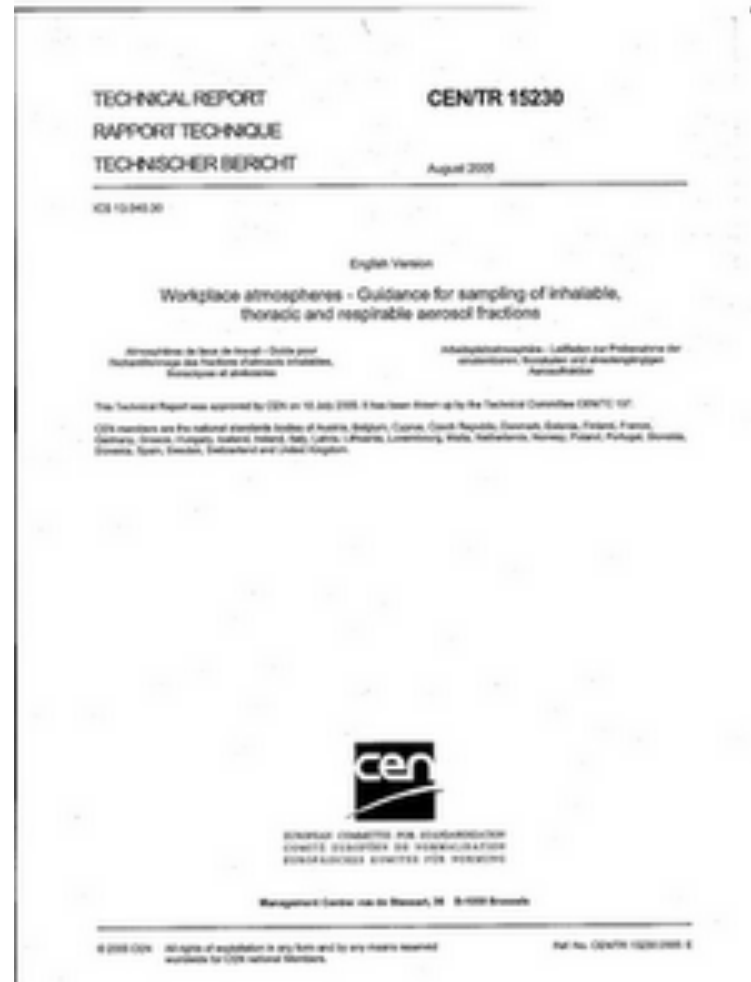


Signed checks



HP Webscan

What we
found...




Technical
reports





HP Webscan

What we found...

 Department of Community Services
Services for Persons with Disabilities

RESPIRE CARE RECEIPT

Care Coordinator: 

IA # 241283 Client Name: 


For month of: _____, 20____

Respite Care Provider: Name: _____
Address: _____
Phone: _____

Pay type:	Pay Rate	Totals
Approved overnight respite at \$ _____ / day	X _____	days = \$ _____
Approved Hourly Respite at \$ _____ / hr	X _____	hours = \$ _____
		Total amount : \$ _____

Respite Care Provider Signature: _____ Date: _____

Client /Guardian Signature: _____ Date: _____



Forms



HP Webscan



Jim is a Certified Mold Inspector!



HP Webscan

Prevalence

- HP scanners for several years have included Webscan functionality

Risk

- Webscan functionality enabled by default without password protection
- Many networks are misconfigured to expose scanners

Automation

- `http://[Scanner IP]/scan/image1.jpg?id=1&type=4&size=1&fmt=1&time=[epoch time]`
 - Predictable URL path for scanned documents
 - Request above URL every second to retrieve any scanned documents



Photocopiers

“Copy from one, it's plagiarism; copy from two, it's research.”

- Wilson Mizner (1876 - 1933)



Xerox Photocopiers



Shodan Results

- Query → **"Spyglass_MicroServer/2.01FC1"**
- Results → 427
- Server string alone offers unique identifier



Shodan Results

- Query → **"Spyglass_MicroServer/2.00FC4"**
- Results → 32
- Tektronix copiers (Phaser branded copiers sold to Xerox in 1999)



Shodan Results

- Query → **"Xerox_MicroServer/Xerox11"**
- Results → 724
- Xerox Workcentre



Xerox Photocopiers

CentreWare
Internet Services
Phaser 6200



Job Accounting

This page displays the 10 oldest job accounting records. Use the [links](#) at the bottom of the page to view other records. Use the [small-type version](#) for easier printing.

Job Index	Protocol	User Name	Host Name	File Name	Job Name	Pages(Sheets) Printed	Pages(Sides) Printed	Start Time	End Time	Interpreter Duration	Paper Type	Paper size	Cyan Used	Magenta Used	Yellow Used	Black Used
1	AppSocket	Charlie	137.229.71.126	ECE ABET Outcomes & Performance Criteria2011-07.27.xls	ECE ABET Outcomes & Performance Criteria2011-07.27.xls	3	3	7/29/2011 12:28:21	7/29/2011 12:28:23	00:00:02	Plain Paper	Letter	0.0301%	0.0299%	0.0693%	0.0959%
2	IPP	joe	137.229.71.137	IPP_Job	IPP_Job	3	3	7/29/2011 14:13:18	7/29/2011 14:13:22	00:00:04	Plain Paper	Letter	0.0001%	0.0000%	0.0008%	0.0377%
3	AppSocket	Charlie	137.229.71.126	ES Course Instructors.xls	ES Course Instructors.xls	1	1	7/29/2011 15:16:53	7/29/2011 15:16:54	00:00:01	Plain Paper	Letter	0.0002%	0.0000%	0.0012%	0.0126%
4	AppSocket	Charlie	137.229.71.126	ES Course Instructors.xls	ES Course Instructors.xls	1	1	7/29/2011 15:17:03	7/29/2011 15:17:04	00:00:01	Plain Paper	Letter	0.0002%	0.0000%	0.0012%	0.0126%
5	AppSocket	Charlie	137.229.71.126	ES Course Instructors.xls	ES Course Instructors.xls	1	1	7/29/2011 15:17:24	7/29/2011 15:17:25	00:00:01	Plain Paper	Letter	0.0002%	0.0000%	0.0012%	0.0126%
6	AppSocket	Charlie	137.229.71.126	ECE ABET Outcomes & Performance Criteria2011-07.27.xls	ECE ABET Outcomes & Performance Criteria2011-07.27.xls	1	1	7/29/2011 15:21:17	7/29/2011 15:21:20	00:00:03	Plain Paper	Letter	0.0100%	0.0100%	0.0231%	0.0320%
7	AppSocket	Charlie	137.229.71.126	Microsoft Word - Monastic Speaker Schedule 2011.doc	Microsoft Word - Monastic Speaker Schedule 2011.doc	3	3	7/30/2011 14:26:58	7/30/2011 14:27:02	00:00:04	Plain Paper	Letter	0.0002%	0.0008%	0.0000%	0.0185%
8	AppSocket	Charlie	137.229.71.126	Microsoft Word - Monastic Speaker Schedule 2011.doc	Microsoft Word - Monastic Speaker Schedule 2011.doc	4	4	7/30/2011 14:27:26	7/30/2011 14:27:29	00:00:03	Plain Paper	Letter	0.0003%	0.0011%	0.0000%	0.0251%
9	AppSocket	Charlie	137.229.71.126	DegreeWorks by SunGard Higher Education DegreeWorks 4.0.7 DGWP UAF	DegreeWorks by SunGard Higher Education DegreeWorks 4.0.7 DGWP UAF	1	1	7/30/2011 16:45:36	7/30/2011 16:45:38	00:00:02	Plain Paper	Letter	0.0003%	0.0002%	0.0003%	0.0012%

Job Accounting

- File name
- User name
- Pages
- Date
- Time



Xerox Photocopiers

XEROX CentreWare Internet Services
Phaser 6200

More Printers Index Help

Status Jobs Print Properties Troubleshoot Support

```
220 FTP server ready.  
Name [redacted]:Michael):  
230 Password not required for Michael.  
Remote system type is ececolor.  
ftp> pwd  
Remote directory: PRINTER:/  
ftp>
```

FTP Settings
You can retrieve job accounting records and send print ready files to the printer via the FTP protocol.

FTP

Login Password

Page Description Language

Filtering

Job Pipelining

Need a place to store your warez?

- FTP server enabled by default
- No password

Phaser 6200

- About Printer
- General
 - Printer Defaults
 - Date and Time
 - Warmup
 - Usage Profile Properties
 - Resets
- E-Supplies
- Mail Alerts
- Interfaces
- Protocols
 - TCP/IP
 - Port 9100
 - LPR
 - IPP
 - SNMP
 - FTP**
 - Email Server
 - Remote Printing

Name: ececolor
DNS: DUCK-205-X6200-1.printers.uaf.edu
IP: 137.229.37.132



Xerox Photocopiers

XEROX **CentreWare**
Internet Services

Phaser 6200

Features
Premium Color Printing- up to 1200 DPI
Outstanding Speed- 16 pages per minute
Fast Warm-up and first page out
Easy to replace supplies
High Performance built-in PostScript 3 processor
Up to 512 MB RAM

Optional Features
(√ = installed on this printer)
√ Duplexer
Lower Tray Deck
Hard Drive

E Mail Features
Email Alerts (MailInX)
Email Remote Print

Printer Drivers
[Install Printer Drivers](#)
<http://www.evil.com/>

Printer Status
MPT Is Empty

Contact:
Name: ececolor
DNS: DUCK-205-X6200-1.printers.uaf.edu
IP: 137.229.37.132
Location:
Status: Error

Refresh Status

Tektronix
COLOR PRINTERS BY
XEROX

COPYRIGHT © 2001 XEROX CORPORATION. All Rights Reserved.

Status **Jobs** **Print** **Properties** **Troubleshoot** **Support**

Phaser 6200

About Printer

General

- Printer Defaults
- Date and Time
- Warmup
- Usage Profile Properties
- Resets

Supplies

Mail Alerts

Interfaces

Protocols

- TCP/IP
- Port 9100
- LPR
- IPP
- SNMP
- FTP
- Email Server
- Remote Printing
- EtherTalk
- NetWare

Web Links

The Web Links page contains special links to Xerox internet sites so that you can easily access printer documentation, software, service and supplies. Alternatively, you can enter custom URLs in the fields below to access your own network files or internet for desired content.

In the fields below, select "Xerox link" to continue using the default links, or select "Custom link" and enter your custom URL.

Software Links

Printer Drivers

Xerox® link Custom link :

Other Printer Software

Xerox® link Custom link :

Documentation Links

User Manuals & Videos

Xerox® link Custom link :

Support Links

Supplies

Xerox® link Custom link :

Home Server

Home Server Name

Home Server URL

Save Changes **Discard Changes**

Sharp Photocopiers

Document Administration Function

Data Forward to Administrator

Enable

Forwarding Destination Settings

Notice: Address configured as forward address cannot be deleted from the address book.

E-mail

Direct Entry

Global Address Search (G)

ACTION: Demonstrate how to use the Document Administration Function. This function is used to forward all data transmitted and received by the machine to a specified destination.

BENEFIT: Allowing administrators to monitor and archive inbound and outbound communications is an important security feature for protecting valuable company information. This function also gives administrators the ability to choose which destination (E-mail Address, FTP, Network folder or Desktop) to store their forwarded data according to their company's storage needs.

Select Data to be Forwarded

Forward All Received Data

Forward All Send Data

Print Style Setting

Always print

Print at Error

- MENU -

MX-M450U

System Information

- [Device Status](#)
- [Device Configuration](#)
- [Network Status](#)

Image Send Management

- [Destination](#)
- [Sender](#)

Link

Device Management

- [Fax Memory Box](#)
- [Account Control](#)
- [Paper Type](#)
- [Storage Backup](#)



Ricoh Photocopiers

Shodan Results

- Query → “Web-Server/3.0”
- Results → 19,252
- Server string alone offers unique identifier

unique identifier

- server string alone offers

```
HTTP/1.0 200 OK
Date: Sun, 24 Apr 2011 06:26:01 GMT
Server: Web-Server/3.0
Content-Type: text/html; charset=UTF-8
Content-Length: 304
Pragma: no-cache
Set-Cookie: cookieOnOffChecker=on; path=/
Connection: close
```



Ricoh Photocopiers

RICOH Aficio MP C4000

Home | Document Server | Fax Received File | Printer: Print Jobs | Job | Configuration

Home

Cache of previously copied documents

Details of received/transmitted faxes

English | Refresh

Status | Device Info | Counter | Inquiry

- Device Name - RICOH Aficio MP C4000
- Location
- Communication
- Host Name

Status		
Printer	Energy Saver Mode	>>>
Copier	Energy Saver Mode	>>>
Fax	Energy Saver Mode	>>>
Scanner	Alert	>>>

Printer:
Energy Saver Mode



Ricoh Photocopiers

Note to Administrator

This manual is intended to provide administrators with additional information about the security functions of this printer. Read this manual as well as "Software Guide".

This manual and its contents should be kept by, and restricted to, administrators.

Password

When you log on to this printer, you will be prompted to enter the user name and password or access code for your account. We strongly recommend you to change the factory default user name and create a password or an access code immediately to prevent information leakage and unauthorized operations by others.

You will be prompted to enter your login password or access code when performing the following operations:

- Logging on to Administrator mode in Web Image Monitor
- Changing printer settings for an administrator using Smart Organizing Monitor

To use the default account, enter "admin" as the user name, and leave the password blank when using Web Image Monitor. When using Smart Organizing monitor, enter "admin" as the access code.

To Change password for Web Image Monitor and Smart Organizing Monitor, you need to log on as an Administrator, and then make the necessary settings.

Reference

For details about setting a password, see Web Image Monitor or Smart Organizing Monitor Help.

Note to Administrator

This manual is intended to provide administrators with additional information about the security functions of this printer. Read this manual as well as "Software Guide".

This manual and its contents should be kept by, and restricted to, administrators.

Password

When you log on to this printer, you will be prompted to enter the user name and password or access code for your account. We strongly recommend you to change the factory default user name and create a password or an access code immediately to prevent information leakage and unauthorized operations by others.

You will be prompted to enter your login password or access code when performing the following operations:

- Logging on to Administrator mode in Web Image Monitor
- Changing printer settings for an administrator using Smart Organizing Monitor

To use the default account, enter "admin" as the user name, and leave the password blank when using Web Image Monitor. When using Smart Organizing monitor, enter "admin" as the access code.

To Change password for Web Image Monitor and Smart Organizing Monitor, you need to log on as an Administrator, and then make the necessary settings.

Reference

For details about setting a password, see Web Image Monitor or Smart Organizing Monitor Help.



When user manuals are a click away, default passwords, especially on hardware devices, are as good as no password at all.

Ricoh Photocopiers

RICOH Aficio MP 161 Web Image Monitor

Configuration

- Home
- Job
- Address Book
- Configuration

Device Settings

- System
- Paper
- Date/Time
- Timer
- Logs
- E-mail
- Auto E-mail Notification
- On-demand E-mail Notification
- File Transfer
- User Authentication Management
- Administrator Authentication Management
- Program/Change Administrator
- LDAP Server
- Firmware Update

Printer

- Basic Settings
- Tray Parameters (PCL)

Fax

- General
- Administrator Tools
- E-mail Settings
- IP-Fax Settings
- IP-Fax Gateway Settings
- Parameter Settings

Interface

- Interface Settings

Network

- IPv4
- IPv6
- NetWare

Security

- Network Security
- Access Control
- IPP Authentication
- SSL/TLS
- ssh**
- Site Certificate
- Device Certificate

Extended Feature Settings

- Startup Setting
- Extended Feature Info
- Install
- Uninstall
- Administrator Tools
- Copy Extended Features
- Copy Card Save Data

[▲ To Top](#)



Ricoh Photocopiers

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-07-20
Nmap scan report for [REDACTED]
Host is up (0.13s latency).
Not shown: 976 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
23/tcp    open      telnet
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   open      netbios-ssn
340/tcp   filtered  unknown
445/tcp   filtered  microsoft-ds
514/tcp   open      shell
515/tcp   open      printer
593/tcp   filtered  http-rpc-epmap
631/tcp   open      ipp
902/tcp   filtered  iss-realsec
1137/tcp  filtered  unknown
1524/tcp  filtered  ingreslock
2034/tcp  filtered  scoremgr
3914/tcp  filtered  unknown
4444/tcp  open      krb524
5190/tcp  open      aol
6692/tcp  filtered  unknown
7443/tcp  open      unknown
9100/tcp  open      jetdirect
12174/tcp filtered  unknown
30000/tcp filtered  unknown
51493/tcp filtered  unknown
```

```
Michael-Suttons-MacBook-Pro-2:~ Michael$ telnet [REDACTED]
Trying [REDACTED]:
Connected to [REDACTED].
Escape character is '^]'.

RICOH Maintenance Shell.
```

```
Michael-Suttons-MacBook-Pro-2:~ Michael$ ftp [REDACTED]
Connected to [REDACTED].
220 RICOH Aficio MP 161 FTP server (6.11) ready.
Name (66.232.194.15:Michael): admin
331 Password required for admin.
Password:
230 User admin logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65532|)
150 Opening ASCII mode data connection for '/'.
-r--r--r-- root root 200 Jan  1 01:08 help
-r--r--r-- root root 200 Jan  1 01:08 info
-r--r--r-- root root 200 Jan  1 01:08 prnlog
-r--r--r-- root root 200 Jan  1 01:08 stat
-r--r--r-- root root 200 Jan  1 01:08 syslog
-r--r--r-- root root 200 Jan  1 01:08 version.txt
-r--r--r-- root root 200 Jan  1 01:08 errlog.txt
226 Transfer complete.
ftp> █
```

```
devicename  change device name
upnp        configure UPnP parameters
ssdp        configure SSDP parameters
lpr         configure LPR parameters
ipv6        configure IPv6 parameters
ssh         configure ssh/sftp parameters
msh> █
```



Ricoh Photocopiers – Faxes Received

NRG DSm415

English

Top Page

Administrator Mode

Help

URL

Fax Journal: Reception

» Status

» Job

» Printer

» Job History

» Error Log

» Fax History

» Transmission

» Reception

» LAN-Fax

» Configuration

Download Reception List

Refresh

Search for : Unspecified : Search

Page : Go Display items : 10

Date	Details	Destination	Line	Page(s)	Result	User Name	Document No.
6/5/2011 14:30			G3	1	OK		1861
28/4/2011 21:04			G3	8	OK		1858
18/4/2011 10:29			G3	1	OK		1855
18/4/2011 9:34			G3	1	OK		1853
14/4/2011 14:57			G3	2	OK		1850
29/3/2011 6:12			G3	1	OK		1843
29/3/2011 6:07			G3	1	OK		1841
4/3/2011 14:39			G3	2	OK		1835
4/3/2011 13:32			G3	2	OK		1833
3/3/2011 7:55			G3	2	OK		1830



Ricoh Photocopiers – Document Server

The screenshot displays the Ricoh LANIER LD151 Web Image Monitor interface. The top navigation bar includes links for 'To Link Page', 'Version Information', and 'Help'. The main header shows 'LANIER LD151 Web Image Monitor' and a language selector set to 'English'. A left sidebar contains navigation options: 'Login', 'Top Page', 'Status', 'Document Server', 'Job', 'Inquiry', and 'Configuration'. The main content area is titled 'Document Server File List' and features a 'Refresh' button. Below this are search and view controls, including a search box, a 'Search' button, and options for 'View' (set to 'All'), 'Display items' (set to '12'), and 'Display method' (set to 'Thumbnails'). A summary bar indicates 'Total Files : 11 Selected Files : 0' with an 'Uncheck All' button and 'Columns : 4'. The file list table has columns for 'File name', 'User name', 'Created', and 'Expires'. The first row shows files 'SCAN0005', 'SCAN0004', 'SCAN0001', and 'COPY0015'. The second row shows 'COPY0014', 'COPY0017', 'SCAN0003', and 'SCAN0002'. Each file entry includes a thumbnail and a 'Thumbnails (Password)' label. Action icons for 'SCAN' and 'COPY' are visible above each file name.

LANIER LD151 Web Image Monitor

To Link Page > Version Information > ? Help

English Keyword Search

Login

Document Server File List

Print Delete Refresh

View : All Search for : Unspecified Search

1/1 Page : Go Display items : 12 Display method : Thumbnails

Total Files : 11 Selected Files : 0 Uncheck All Columns : 4

	File name	User name	Created	Expires
Thumbnails (Password)	SCAN0005	SCAN0004	SCAN0001	COPY0015
Thumbnails (Password)	COPY0014	COPY0017	SCAN0003	SCAN0002

- Previously copied document available via a web based interface



Ricoh Photocopiers – Document Server

LANIER LD151
Web Image Monitor

To Link Page > Version Information > ? Help

English Keyword Search

Login

- Top Page
- Status
- Document Server
- Job
- Inquiry
- Configuration

File Properties

Enlarge Image

Only image of first page will be enlarged.

File name : SCAN0001

User name :

Created : Mar 17, 2009 12:44:22 AM

Expires : Unspecified

Storing method : Scanner

Page(s) : 1

Scan size : 8 1/2 x 11

File size : 186KB

Resolution : 200 dpi

Scan type : Black & White: Text

Password : Off

Download

File format : PDF

Page : All
 Specify
E.g. 1,3,6,8-10
Specify one page only for JPEG.

Download

- Available for download in PDF/TIFF formats



Security Systems

*“Who controls the past controls the future.
Who controls the present controls the past.”*

- George Orwell (1903 - 1950)



Security Systems



Control panel with the following elements from top to bottom:

- Close button (square icon)
- Grid view button (4 squares icon)
- Refresh button (circular arrow icon)
- Auto button
- Channel selector: 1 (with up/down arrows)
- Refresh button (text)
- Logout button (text)



Webcams

LINKSYS
A Division of Cisco Systems, Inc.

WVC54GCA

Wireless-G Internet Home Monitoring Camera

Home | View Video | Linksys Web | Help | Exit

Setup

- Basic
- Image
- Administration
- Users
- Options
- Motion Detection**
- Status

Motion Detection Settings

Trigger Motion Detection

Enable Motion Detection:

Attachment Type: JPEG Image

Frame Rate: 1 fps

Pre-Capture Length: 0 Second(s)


Post-Capture Length: 1 Second(s)

Interval: 15 Minute(s) before detecting the next motion detection.

Action(s): E-Mail FTP

Send To: [Redacted]@aol.com (E-Mail Address #1)
[Redacted] (E-Mail Address #2)

Apply Cancel Help



Networking

“I hear there's rumors on the Internets that we're going to have a draft.”

- George W. Bush (Oct. 8, 2004)



Cisco

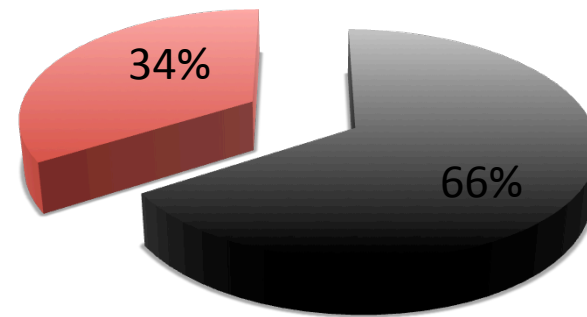
Shodan Results

- Query → “Server: cisco-IOS”
- Results → 429,736
- All of the first 50 results are either password protected, or inaccessible

Shodan Results

- Query → “Server: cisco-IOS”
“200 OK”
- Results → 12,239
- 33 of the first 50 results were not password protected

```
HTTP/1.0 200 OK
Date: Sat, 31 Jul 1993 21:26:32 UTC
Server: cisco-IOS/12.1 HTTP-server/
1.0(1)
Mime-version: 1.0
Pragma: no-cache
content-type: text/html
```



■ No Password ■ Password/Inaccessible



Cisco

Purpose

- Manage devices
- Monitor device health

Observations

- Numerous UIs identified with varying degrees of functionality
- Many are clearly dated, based on copyright © and browser identification (i.e. Netscape 7.0)
- Initial 'router web setup' screens often encountered

Risk

- Reconfigure devices
- Reroute traffic
- DoS



Cisco Catalyst Switch

CISCO SYSTEMS



Close Window

Toolkit: Roll over tools below



Cisco

HOME

EXPRESS SETUP

CLUSTER
MANAGEMENT SUITE

TOOLS

HELP RESOURCES

Home: Master Summary Status

Network Identity

IP Address

MAC Address

00:0F:34:CF:3D:00

System Details

Host Name

SW-NDC-3750

System Uptime

24 weeks, 2 days, 15 hours, 17 minutes

Serial Number

CAT0810N078

Software Version

12.1(19)EA1d

System Contact

noc()bluemediacommlcom

System Location

Cebu

Refresh



Close Window

Copyright (c) 2003 by Cisco Systems, Inc.

Cisco Catalyst 2960 Series

Catalyst 2960 Series Device Manager - SI.Structis.1.026

Language: English

Session: Standard | Secured

Refresh Print Smartports Software Upgrade Legend Help



Uptime: 12 weeks, 5 days, 16 hours, 12 minutes

Next refresh in 59 seconds

View: Status



Move the pointer over the ports for more information.

Contents

- Dashboard
- Configure
- Monitor
- Maintenance
- Network Assistant

Dashboard

Switch Information

Host Name: SI.Structis.1.026
Product ID: WS-C2960G-8TC-L
IP Address: 89.81.170.206
MAC Address: E8:04:62:A3:79:80
Version ID: V02
Serial Number: FOC1432V687
Software: 12.2(44)SE6
Contact:
Location:

Switch Health

View Trends

Bandwidth Used



0%

Packet Error



0%

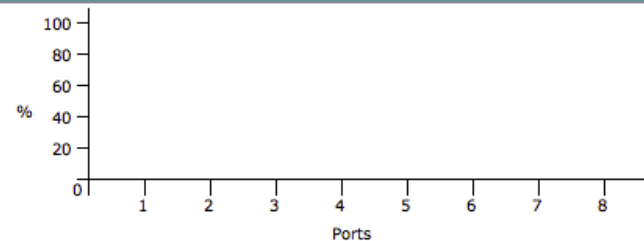
Temp



36 °C
OK

Port Utilization

View Trends | View Port Statistics



Legend: Receive Transmit



Cisco Catalyst Switch

CISCO SYSTEMS Close Window Toolkit: Roll over tools below

Cisco

HOME
EXPRESS SETUP
CLUSTER MANAGEMENT SUITE
TOOLS
HELP RESOURCES

Express Setup

Management Interface: VLAN1 - Default

IP Address: IP Subnet Mask: 128.0.0.0

Default Gateway:

Switch Password: Confirm Switch Password:

Optional Settings

Host Name: SW-NDC-3750

System Contact: noc()bluemediaacor System Location: Cebu

Telnet Access: Enable Disable

Telnet Password: Confirm Telnet Password:

SNMP: Enable Disable

SNMP Read Community: bluecheck99 SNMP Write Community:

Save Cancel

Change switch password/change routing

Enable telnet access and change password

Enable SNMP access and change password



Cisco Catalyst Switch

Command

Output

Command base-URL was: /exec/
Complete URL was: /exec/

Exec commands:

[access-enable](#)
Create a temporary Access-List entry

[access-template](#)
Create a temporary Access-List entry

[archive](#)
manage archive files

[cd](#)
Change current directory

[clear](#)
Reset functions

[clock](#)
Manage the system clock

[configure](#)
Enter configuration mode

[copy](#)
Copy from one file to another

[debug](#)
Debugging functions (see also 'undebug')

[delete](#)
Delete a file

[dir](#)
List files on a filesystem

[dot1x](#)
Dot1x Exec Commands

[erase](#)
Erase a filesystem

[format](#)
Format a filesystem

[fsck](#)
Fsck a filesystem

- Web based command line interface
- Can be leveraged to completely reconfigure the device or obtain configuration information



Cisco Catalyst Switch

Ping

Protocol:

Destination: (n.n.n.n)

Source interface:

Multicast interface:

Repeat Count:

Timeout (seconds):

Datagram Size:

Time To Live:

Type of Service:

Verbose:

Set DF bit in IP Header:

Validate Reply Data:

- Web based ping tool
- Also makes for a handy network scanner to identify otherwise inaccessible hosts



Cisco Catalyst Switch

Contents

- Dashboard
- ▼ Configure
 - Smartports
 - Port Settings
 - Express Setup
 - Restart / Reset
- ▶ Monitor
- ▼ Maintenance
 - Telnet
 - Software Upgrade
- Network Assistant

Software Upgrade

The switch is running Cisco IOS software release: 12.2(44)SE6

- Go to <http://www.cisco.com/public/sw-center/> to find the latest Cisco IOS software (in tar file format) for the switch.
- Download the tar file to your PC or to a network drive.
- Select the tar file to upgrade using the Browse... button.
- Click Upgrade.

Image File Name: no file selected



- Install a custom (backdoored) version of IOS

VoIP

“Well, if I called the wrong number, why did you answer the phone?”

- James Thurber (1894 - 1961), New Yorker cartoon caption, June 5, 1937



VoIP

Purpose

- Manage devices – security, logging, networking, etc.
- Debugging – run diagnostics

Risk

Vendor	Product	Server Headers	ShodanHQ
Polycom	Soundpoint	Polycom SoundPoint IP Telephone HTTPd	6,737
Polycom	CMA	Apache	N/A
3Com	NBX	Virata-EmWeb/R6_0_3	1,351
Snom	Various	snom embedded	1,114



Polycom SoundPoint

POLYCOM Polycom VoIP SoundPoint IP Configuration Utility

[Home](#) [Core Conf.](#) [Sip Conf.](#) [Registration](#)

Registration Parameters:

[Registration 1](#) [Registration 2](#) [Registration 3](#) [Registration 4](#) [Registration 5](#) [Registration 6](#)

Registration 1	
Identification	
Display Name	HY
Address	1104
Auth User ID	1104
Auth Password	*****
Label	1104
Type	<input checked="" type="radio"/> Private <input type="radio"/> Shared
Third Party Name	
Server 1	
Address	
Port	
DNS Lookup	DNSnaptr
Expires	
Register	
Retry Time Out	
Retry Max Count	
Line Seize Time Out	



Sipura SPA-2000

SIPURA
technology, inc.

Sipura Phone Adapter Configuration

Info **System** SIP Provisioning Regional Line 1 Line 2 User 1 User 2 [User Login](#) [basic](#) | [advanced](#)

System Configuration

Restricted Access Domains:

Enable Web Server: yes no
Enable Web Admin Access: yes no
User Password:

Web Server Port:
Admin Passwd:

Internet Connection Type

DHCP:
Static IP: NetMask:
Gateway:

Optional Network Configuration

HostName: Domain:
Primary DNS: Secondary DNS:
DNS Server Order: DNS Query Mode:
Syslog Server: Debug Server:
Debug Level: Primary NTP Server:
Secondary NTP Server:

[User Login](#) [basic](#) | [advanced](#)



Snom

Welcome to Your Phone!

VERSION 8

Operation

Home
Directory

Setup

Preferences
Speed Dial
Function Keys
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Certificates
Software Update

Status

System Information
Log
SIP Trace
DNS Cache
Subscriptions
PCAP Trace
Memory
Settings

Manual



Did you know, that...

- you can customize the screen of your snom phone?
- you can even open doors with your snom phone?

...and much more? - [Read more](#)

This web interface makes it easy for you to set your phone up correctly and to access the advanced features. To dial a number, just enter the number in the field below. You can enter a simple telephone number (e.g. 0114930398330) or URI like info@snom.com.

Dial a Number:

Dial Hangup

Outgoing Identity:

7104@192.168.3.203 Set

Make Calls

[Dialed](#), [Missed](#), [Received](#)

Dialed Numbers ✕

Date	Time	Duration	Costs	Local Identity	Number
4/29/2011	14:45	0:23		7104@192.168.3.203	
4/29/2011	14:31	0:07		7104@192.168.3.203	
4/29/2011	11:09	3:34		7104@192.168.3.203	
4/29/2011	10:56	3:33		7104@192.168.3.203	
4/29/2011	08:56	0:04		7104@192.168.3.203	
4/28/2011	15:56	0:01		7104@192.168.3.203	
4/28/2011	15:55	0:00		7104@192.168.3.203	
4/28/2011	10:33	0:33		7104@192.168.3.203	
4/27/2011	14:30	0:30		7104@192.168.3.203	
4/27/2011	14:24	1:09		7104@192.168.3.203	
4/27/2011	11:10	5:04		7104@192.168.3.203	
4/27/2011	10:04	1:16		7104@192.168.3.203	
4/25/2011	10:46	10:24		7104@192.168.3.203	
4/25/2011	10:45	10:54		7104@192.168.3.203	
4/25/2011	10:45	0:00		7104@192.168.3.203	

Call history

Various debugging tools



snom

Snom

Welcome to Your Phone!

VERSION 7

HTTP Password not set!

Operation

Home
Directory

Setup

Preferences
Speed Dial
Function Keys
Identity 1
Identity 2
Identity 3
Identity 4
Action URL Settings
Advanced
Trusted Certificates
Software Update

Status

System Information



Did you know, that...

- you can customize the screen of your snom phone?
- you can even open doors with your snom phone?

...and much more? » [Read more](#)

This web interface makes it easy for you to set your phone up correctly and to access the advanced features.

To dial a number, just enter the number in the field below. You can enter a simple telephone number (e.g. 0114930398330) or URI like info@snom.com.

Dial a Number:

Outgoing Identity:

HTTP:

User:

Password:

Authentication Scheme:

Digest Basic

HTTP Proxy:

HTTP port:

80

HTTPS port:

443

Register HTTP contact:

on off

Webserver connection type:

http or https

Auto Logout (min):

Setup → Advanced → HTTP



Snom SIP Trace


SIP Trace

Operation
Home
Directory

Setup
Preferences
Speed Dial
Function Keys
Advanced

Status
System Information
Log
SIP Trace
DNS Cache
Subscriptions
PCAP Trace
Memory

Manual


© 2000-2008 [snom AG](#)

[Clear](#) [Reload](#)

Received from udp:208.24.218.117:5060 at 29/4/2011 16:44:12:304 (245 bytes):

```
OPTIONS sip:67.20.0.124:1031 SIP/2.0
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=0
From: sip:ping@sbcmegagate.com;tag=0d3df4b9
To: sip:67.20.0.124:1031
Call-ID: 14ed0877-4a0e5868-737306@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```

Sent to udp:208.24.218.117:5060 at 29/4/2011 16:44:12:316 (539 bytes):


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=0
From: sip:ping@sbcmegagate.com;tag=0d3df4b9
To: sip:67.20.0.124:1031
Call-ID: 14ed0877-4a0e5868-737306@208.24.218.117
CSeq: 1 OPTIONS
Contact: <sip:6014133512@10.10.11.7:2048;line=kygs41of>;flow-id=1
User-Agent: snom320/7.1.39
Accept-Language: en
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
Allow-Events: talk, hold, refer, call-info
Supported: timer, replaces, from-change
Content-Length: 0
```

Received from udp:208.24.218.117:5060 at 29/4/2011 16:44:27:311 (245 bytes):

```
OPTIONS sip:67.20.0.124:1031 SIP/2.0
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=0
From: sip:ping@sbcmegagate.com;tag=f4adf4b9
To: sip:67.20.0.124:1031
Call-ID: 14ed0877-327e5868-647306@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```

Sent to udp:208.24.218.117:5060 at 29/4/2011 16:44:27:323 (539 bytes):

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=0
From: sip:ping@sbcmegagate.com;tag=f4adf4b9
To: sip:67.20.0.124:1031
Call-ID: 14ed0877-327e5868-647306@208.24.218.117
CSeq: 1 OPTIONS
Contact: <sip:6014133512@10.10.11.7:2048;line=kygs41of>;flow-id=1
User-Agent: snom320/7.1.39
Accept-Language: en
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
Allow-Events: talk, hold, refer, call-info
Supported: timer, replaces, from-change
Content-Length: 0
```



Snom PCAP Trace

PCAP Trace

Operation

Home
Address Book

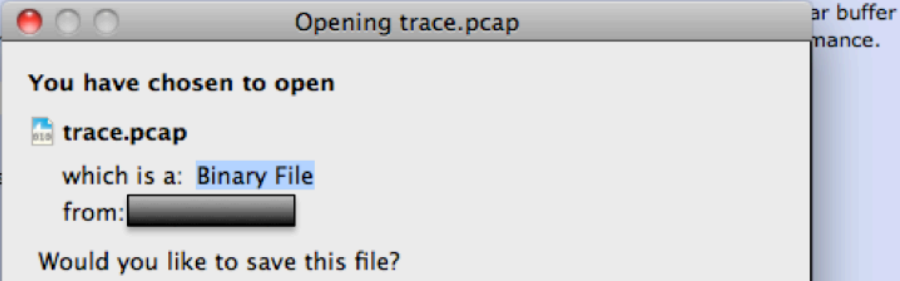
Setup

Preferences
Speed Dial
Function Keys
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Trusted Certificates
Software Update

To see what is going on on the network level, you can generate PCAP files on this page. These files can be read with various network tools, for example Ethereal. To start recording, press the start button and to stop recording, press the stop button. (to avoid overflow of the buffer)

Start Stop

Click [here](#) to save



Web Interface/V8/PCAP Trace

< Web Interface | V8

Languages: English • Deutsch

On this page you can create IP packet traces from current network traffic directly on your phone. This tool is very powerful in order to analyze the network traffic on the phone's ethernet interface.

Description	Screenshot
<ul style="list-style-type: none">By pressing the "start" button, trace recording will start recording every incoming or outgoing packet addressed to/from your phonePressing the "stop" button will stop trace recording.By clicking on the "here" link the trace will be saved into the specified file. That file with the extension "pcap" can be easily analyzed with tools like Ethereal or Wireshark or.	<p>Um zu sehen, was auf Netzwerkebene vorgeht, können hier PCAP Dateien generiert werden. Diese Dateien können von verschiedensten Netzwerktools (z.B. wireshark) eingelesen werden. Um die Aufzeichnung zu beginnen, drücken Sie den Startknopf und um die Aufzeichnung zu stoppen, den Stopknopf. Bitte bedenken Sie dabei, daß die Daten in einem Ringpuffer gespeichert werden (um Überläufe zu verhindern) und das die Aufnahme eventuell negativen Einfluß auf die Performance des Gerätes haben kann.</p> <p>Start Stop</p> <p>Klicken Sie hier um den aktuellen PCAP Trace zu speichern. (0 packets, 0 octets).</p>



3Com NBX



Shodan Results

- Query → “Server: Virata-EmWeb/R6_0_3”
- Results → 1,362

3Com NBX 100

NBX NetSet™
Administration Utility

3COM

Version: R5_0_23
Created: Aug 3 2006

Logon as:

Administrator

User

```
HTTP/1.0 200 OK
Date: Fri, 08 Jul 2011 00:45:42 GMT
Server: Virata-EmWeb/R6_0_3
Transfer-Encoding: chunked
Content-Type: text/html
Expires: Fri, 08 Jul 2011 00:45:42 GMT
Last-Modified: Fri, 08 Jul 2011 00:45:42 GMT
Cache-Control: no-cache
Pragma: no-cache
```



3Com NBX



Shodan Results

- Query → “Server: Virata-EmWeb/R6_0_3”
- Results → 1,362



```
HTTP/1.0 300 Multiple Choices
Date: Thu, 07 Jul 2011 23:19:15 GMT
Server: Virata-EmWeb/R6_0_3
Transfer-Encoding: chunked
Content-Type: text/html
Expires: Thu, 07 Jul 2011 23:19:15 GMT
Last-Modified: Thu, 07 Jul 2011 23:19:15 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Location: /
TCN: list
Alternates: {"/index.it.html" 1.00 {type text/html}}, {"/index.es-mx.html" 1.00 {type text/html}}, {"/index.pt-br.html" 1.00 {type text/html}}
Vary: *
```



3Com NBX

The screenshot displays the 3Com NBX NetSet utility interface. On the left is the 'NBX NetSet - Main Menu' with various configuration options like NBX Messaging, Device Configuration, Dial Plan, Downloads, Help, Operations, Reports, System Configuration, Tab To It, TAPI, User Configuration, and ACD Configuration. Below these are 'Installation Guide' and 'Administrative Guide' buttons. A search bar contains 'vpim' and a 'Go!' button. A table of contents lists 'Rank Title' items such as '100. VPIM', '81. Advanced VPIM Settings', '78. VPIM Control Parameters', '78. VPIM Statistics', '75. VPIM Operations Management', '13. NBX Messaging', and '2. Group List'. The main window is titled 'NBX Messaging' and has tabs for 'Group List', 'NBX Voice Mail', 'Auto Attendant', and 'VPIM'. The 'VPIM' tab is active, showing a table with columns for 'Local Message Server' and 'Default'. The table contains settings for 'Max message size (Kbs)', 'Time between send attempts (mins)', 'Max number of send attempts', and 'Max time before message expires (mins)'. Below the table is a help page for 'VPIM' with a red-bordered text box containing the definition: 'The Voice Profile for Internet Mail (VPIM) enables users to have their voice mail messages automatically forwarded to an email address. The message is sent as a .WAV file attachment. Users can configure and enable this feature in the Off Site Notification section of the NBX NetSet utility.' Below this is a paragraph about configuring VPIM parameters and a list of links: 'Control Parameters', 'Operations Management', 'Statistics', and 'Advanced Settings'. A 'NOTE' section explains that VPIM uses an SMTP server embedded in the NBX system, which should be protected by a firewall. The footer contains the copyright notice: 'Copyright © 2001-2005, 3Com Corporation. All Rights Reserved.'

NBX NetSet - Main Menu

NBX Messaging

Group List | NBX Voice Mail | Auto Attendant | VPIM

Operations Management

Statistics

Advanced Settings

Local Message Server	Default
Max message size (Kbs):	3000 3000
Time between send attempts (mins):	15 15
Max number of send attempts:	2 4
Max time before message expires (mins):	30 60

VPIM

The Voice Profile for Internet Mail (VPIM) enables users to have their voice mail messages automatically forwarded to an email address. The message is sent as a .WAV file attachment. Users can configure and enable this feature in the Off Site Notification section of the NBX NetSet utility.

Using the NBX NetSet utility, you can configure several VPIM parameters and check VPIM status. See these topics for more information:

- [Control Parameters](#)
- [Operations Management](#)
- [Statistics](#)
- [Advanced Settings](#)

NOTE: VPIM uses an SMTP server that is embedded in the NBX operating system. To avoid abuse by spammers, an SMTP server should always be protected by a firewall. Configure the firewall to allow access to port 25 on the NBX system only from valid VPIM systems that need to deliver VPIM messages to the phone system. The NBX SMTP server is started only when the system has a valid license for VPIM.

Copyright © 2001-2005, 3Com Corporation. All Rights Reserved.

3Com NBX

Setting up NBX 100

1. **SETUP THE PC TO THE SAME IP RANGE WITH THE NBX** >> 192.168.1.x
255.255.255.0
2. **LOGIN TO NBX** through IE
192.168.1.190
user: administrator
password: 0000

System
manual

-
- Security Tips**
- Change your password often.
 - Do not use passwords that can easily identify you, such as your phone extension or birth date.
 - Avoid simple passwords such as 1234 or 0000.
 - Use numbers only; do not use * or # as part of your password.
 - Longer passwords are more secure.
 - Never tell your password to anyone.

User's
guide



3Com NBX



- System-Wide Settings ▶
- Feature Settings ▶
- System Maintenance ▶
- Telephone Configuration ▶
- User Configuration ▶
- Call Distribution Groups ▶
- PSTN Gateway Configuration ▶
- NBX Messaging ▶
- SIP Applications ▶
- Dial Plan ▶
- Virtual Connections ▶
- Downloads ▶
- Licensing and Upgrades ▶
- Reports ▶
- Network Management ▶
- Country Settings ▶

NBX® Version R6_0_63
Copyright © 2006
3Com® Corporation
All Rights Reserved



NBX® V3000

System Maintenance > Call Reporting

Call Reporting

Allows you to configure Call Detail Recording parameters if you do use the CDR application.

Help

Call Detail Recording:

- Disabled
- Enabled with last digits scrambled

CDR Purge Interval: days

- Enabled for XML (recommended)
- Backward compatible for CSV
- Log Internal Calls (if CDR enabled)
- Mark Unrestricted trunk calls as internal
- Also log in XML
- Export data unscrambled

Apply Reset Purge CDR

Detailed logging
can be turned on,
which will record
all phone numbers
dialed from the
system

3Com NBX



- System-Wide Settings ▶
- Feature Settings ▶
- System Maintenance ▶
- Telephone Configuration ▶
- User Configuration ▶
- Call Distribution Groups ▶
- PSTN Gateway Configuration ▶
- NBX Messaging ▶
- SIP Applications
- Dial Plan ▶
- Virtual Connections ▶
- Downloads ▶
- Licensing and Upgrades ▶
- Reports ▶
- Network Management ▶
- Country Settings ▶

NBX® Version R6_0_63
Copyright © 2006
3Com® Corporation
All Rights Reserved



NBX® V3000

System Maintenance > System Backup

System Backup

Backs up the system database, which consists of both end-user and administrator settings and data. The system backs up the database into a compressed file that you can download and store.

[Help](#)

Backup Database

Current Version : R6_0_63

Last Backup : Tue, 5 May 2009 15:27:39

[Download now](#)

System Backup

Include NBX Voice Mail

Include NBX Licenses

[Backup](#)

[Backup All](#)

Include
voicemail in
backup

Download .tar
file
configuration
and data
backup

3Com NBX

- Downloaded .tar archive, contains numerous other .tar archives
- vm.tar stores voicemail messages in alphabetically arranged folders
- File naming convention – vdata###.0
 - This is a .wav file
 - Simply renaming the file with a .wav extension permits playback

That's Brilliant!



Name	Kind
aa.tar	tar archive
data.tar	tar archive
DB.tar	tar archive
etc.tar	tar archive
mail.tar	tar archive
vm	Folder
a	Folder
b	Folder
c	Folder
f	Folder
h	Folder
uid207	Folder
vdata3f5.0	Document
vdata695.0	Document
vdataff6.wav	Waveform audio
uid217	Folder
j	Folder
l	Folder
m	Folder
n	Folder
q	Folder
r	Folder
s	Folder
syslist	Folder
t	Folder
w	Folder
x	Folder
y	Folder
z	Folder



Server Management

“Well, if I called the wrong number, why did you answer the phone?”

- James Thurber (1894 - 1961), New Yorker cartoon caption, June 5, 1937



Server Management - APC

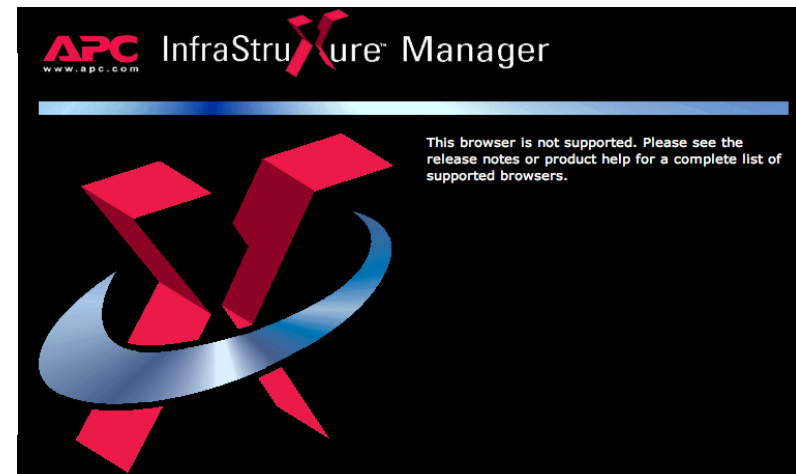


Shodan Results

- Query → **“Server: Acme.Serve/v1.7 of 13nov96”**
- Results → 90
- ActiveX control/Java applet for remotely managing servers/infrastructure

ActiveX control/Java applet for remotely managing servers/infrastructure

```
HTTP/1.0 200 Ok
Date: Sun, 31 Jul 2011 05:00:05 GMT
Server: Acme.Serve/v1.7 of 13nov96
Connection: close
Content-type: text/html
Content-length: 3738
Last-modified: Tue, 06 Nov 2007
20:19:00 GMT
```



Server Management - APC

Shodan Results

- Device: APC NetBotz Appliance
- Query → “**Server: Acme.Serve/v1.7 of 13nov96**”
- Results → 59

Functionality

- Surveillance Cameras
- Environmental alerts
- Stats

HTTP/1.1 200 OK

Server: **thttpd/2.25b 29dec2003**

WWW-Authenticate: **Basic realm="APC Appliance"**

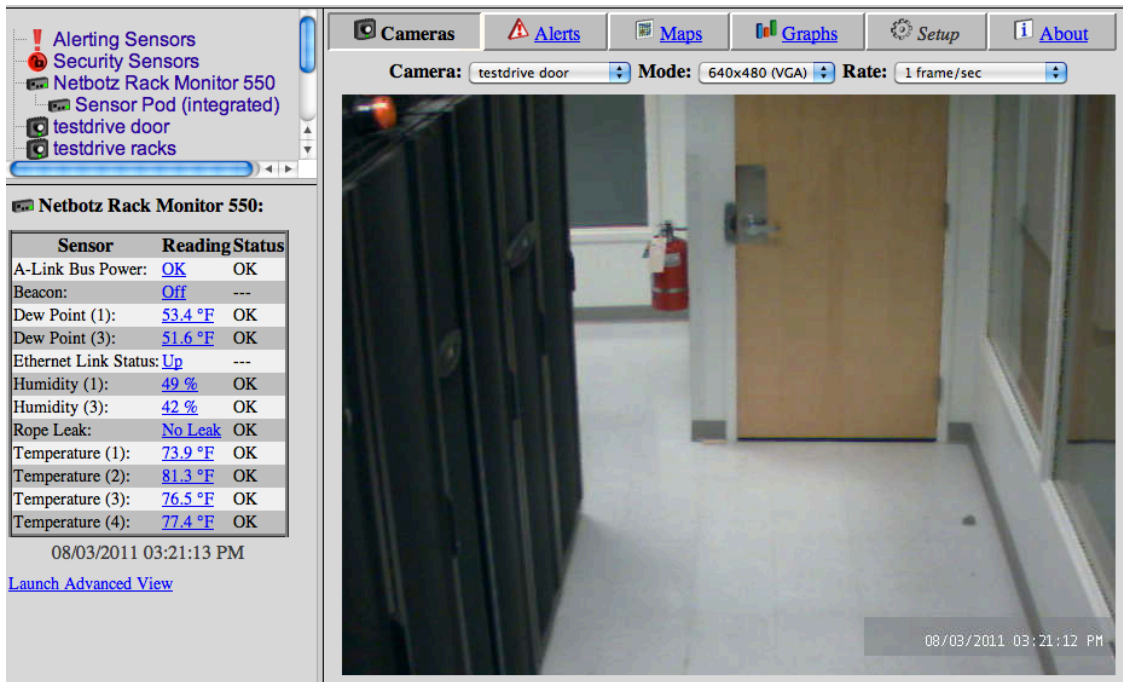
Content-Encoding: gzip

Transfer-Encoding: chunked

Content-Type: text/html; charset=utf-8

Connection: close

Expires: Sat, 01 Jan 2000 12:00:00 GMT



Alerting Sensors
Security Sensors
Netbotz Rack Monitor 550
Sensor Pod (integrated)
testdrive door
testdrive racks

Netbotz Rack Monitor 550:

Sensor	Reading	Status
A-Link Bus Power:	OK	OK
Beacon:	Off	---
Dew Point (1):	53.4 °F	OK
Dew Point (3):	51.6 °F	OK
Ethernet Link Status:	Up	---
Humidity (1):	49 %	OK
Humidity (3):	42 %	OK
Rope Leak:	No Leak	OK
Temperature (1):	73.9 °F	OK
Temperature (2):	81.3 °F	OK
Temperature (3):	76.5 °F	OK
Temperature (4):	77.4 °F	OK

08/03/2011 03:21:13 PM

[Launch Advanced View](#)

Cameras Alerts Maps Graphs Setup About

Camera: testdrive door Mode: 640x480 (VGA) Rate: 1 frame/sec

08/03/2011 03:21:12 PM



Agenda



What can we do about it?



brEWS



The screenshot shows the brEWS web application interface. At the top left is a logo of a beer mug next to the text "brEWS". Below the logo are two buttons: "Scan" and "About". The main content area is titled "Scan IP Address Range for Embedded Web Servers". It contains two input fields: "Starting IP:" and "Ending IP:", with a "Submit" button below them. To the right of the main form is a "Links" section with two links: "Zscaler" and "Zscaler Labs". At the bottom left of the interface, it says "© 2011 Zscaler".

Time to find those pesky EWSs!

Basic Request Embedded Web Server Scanner

<http://brews.zscaler.com>



brEWS

Goal

- Simple, user –friendly, web based scanner for identifying EWSs
- Enable SMBs and consumers – those that may not have security expertise/ personnel to identify potentially exposed devices

Architecture

- LAMP based architecture
- Available online or via downloadable scanning component for identifying LAN based devices

Status

- <http://brews.zscaler.com>
- Feedback – brews@zscaler.com



brEWS

Challenges

- Maintain overall simplicity without compromising needed tests
- Pure client-side scripting deemed not an option due to browser same-origin restrictions

Limitations

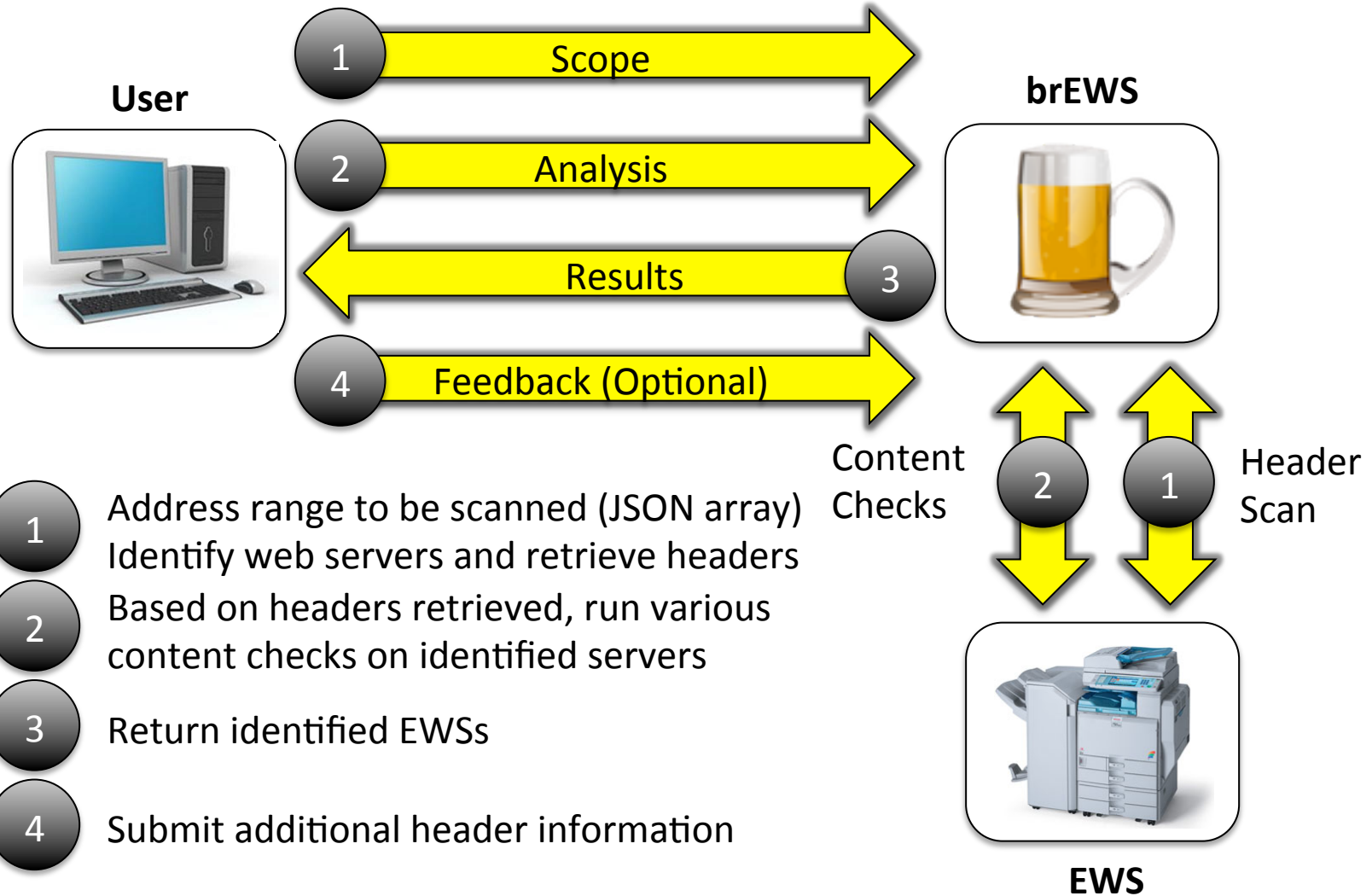
- Assumes unaltered EWS headers
- Local PHP server needed for LAN scanning

Wish List

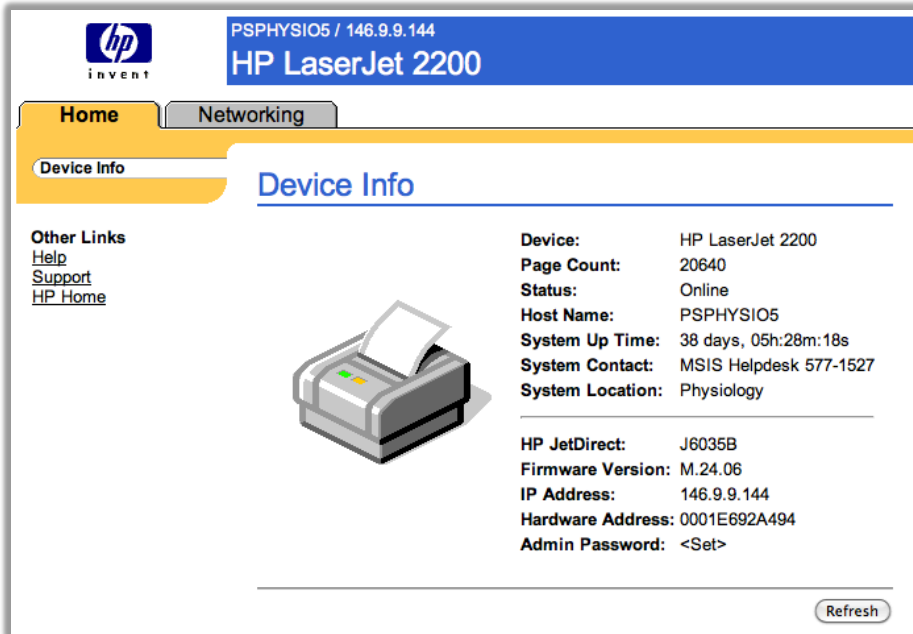
- Expand signature set
 - You can assist → <http://brews.zscaler.com/submit.php>
- Client-side interface – browser plugin/mobile app.
- Expand tests to include known vulnerabilities/



brEWS Process



brEWS Checks – RegEx



The screenshot shows the HP LaserJet 2200 web interface. At the top, there is a blue header with the HP logo and the text "PSPHYSIO5 / 146.9.9.144" and "HP LaserJet 2200". Below the header, there are two tabs: "Home" and "Networking". The "Device Info" section is active, showing a list of links (Other Links) on the left and a table of device information on the right. The table includes fields like Device, Page Count, Status, Host Name, System Up Time, System Contact, System Location, HP JetDirect, Firmware Version, IP Address, Hardware Address, and Admin Password. A printer icon is also visible in the center of the page.

Device:	HP LaserJet 2200
Page Count:	20640
Status:	Online
Host Name:	PSPHYSIO5
System Up Time:	38 days, 05h:28m:18s
System Contact:	MSIS Helpdesk 577-1527
System Location:	Physiology
HP JetDirect:	J6035B
Firmware Version:	M.24.06
IP Address:	146.9.9.144
Hardware Address:	0001E692A494
Admin Password:	<Set>

- Relatively static content across a variety of devices
- Model number displayed in a predictable location/format

Rule

Virata-EmWeb/R6_2_1,regex:/index_info.htm:/hp\\s+\\w*\\s+\\w*/i,HP printer

```
<td width="100%">
<table summary = "This table is used to ...">
<tr>
<td class="clf">Device:</td>
<td class="if">HP LaserJet 2200</td>
</tr>
```



brEWS Checks – Server Response



Rule

Web-Server/3.0,url:/web/guest/en/websys/webArch/authForm.cgi:200,Ricoh photocopier

```
HTTP/1.0 200 OK
Date: Wed, 03 Aug 2011 02:15:15 GMT
Server: Web-Server/3.0
Content-Type: text/html; charset=UTF-8
Expires: Wed, 03 Aug 2011 02:15:15 GMT
...
```

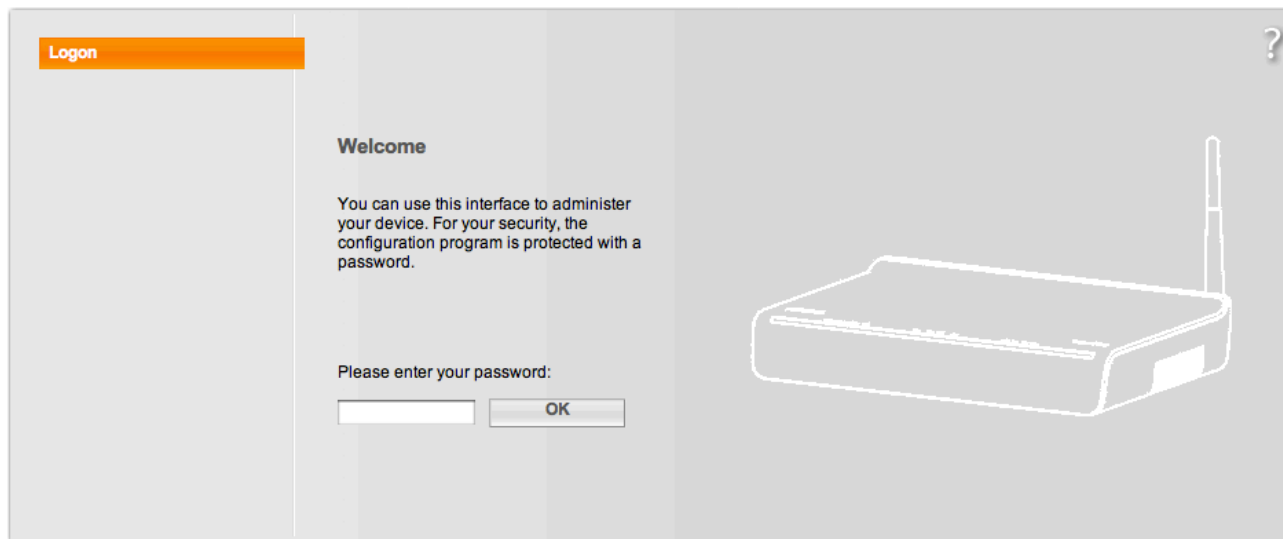
- Combination of page and unique server response is adequate to identify EWS



brEWS Checks – MD5

Gigaset

SX762 WLAN dsl



SIEMENS

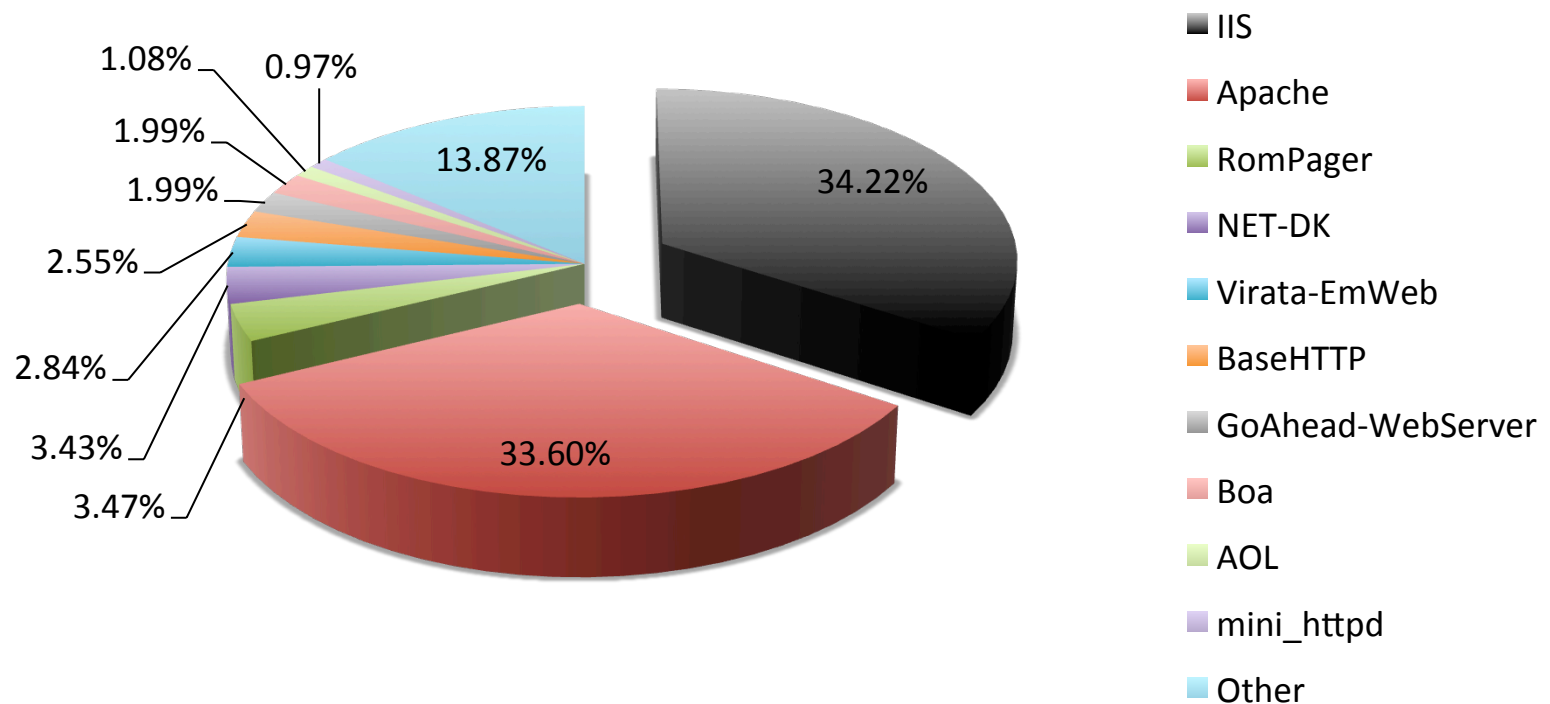
- Model number displayed in image as opposed to text

Rule

SiemensGigaset-Server/1.0,md5:/FS/images/product_name_762.gif:
6353d88288e321d31a572491ce34d6aa,Siemens Gigaset SX762 WLAN DSL



Top 10 Web Servers



- IIS and Apache account for 75%+ of web servers encountered
 - Majority of these would be 'traditional' web servers
- What makes up the remaining 25%?



Unique Servers With 25+ Hits



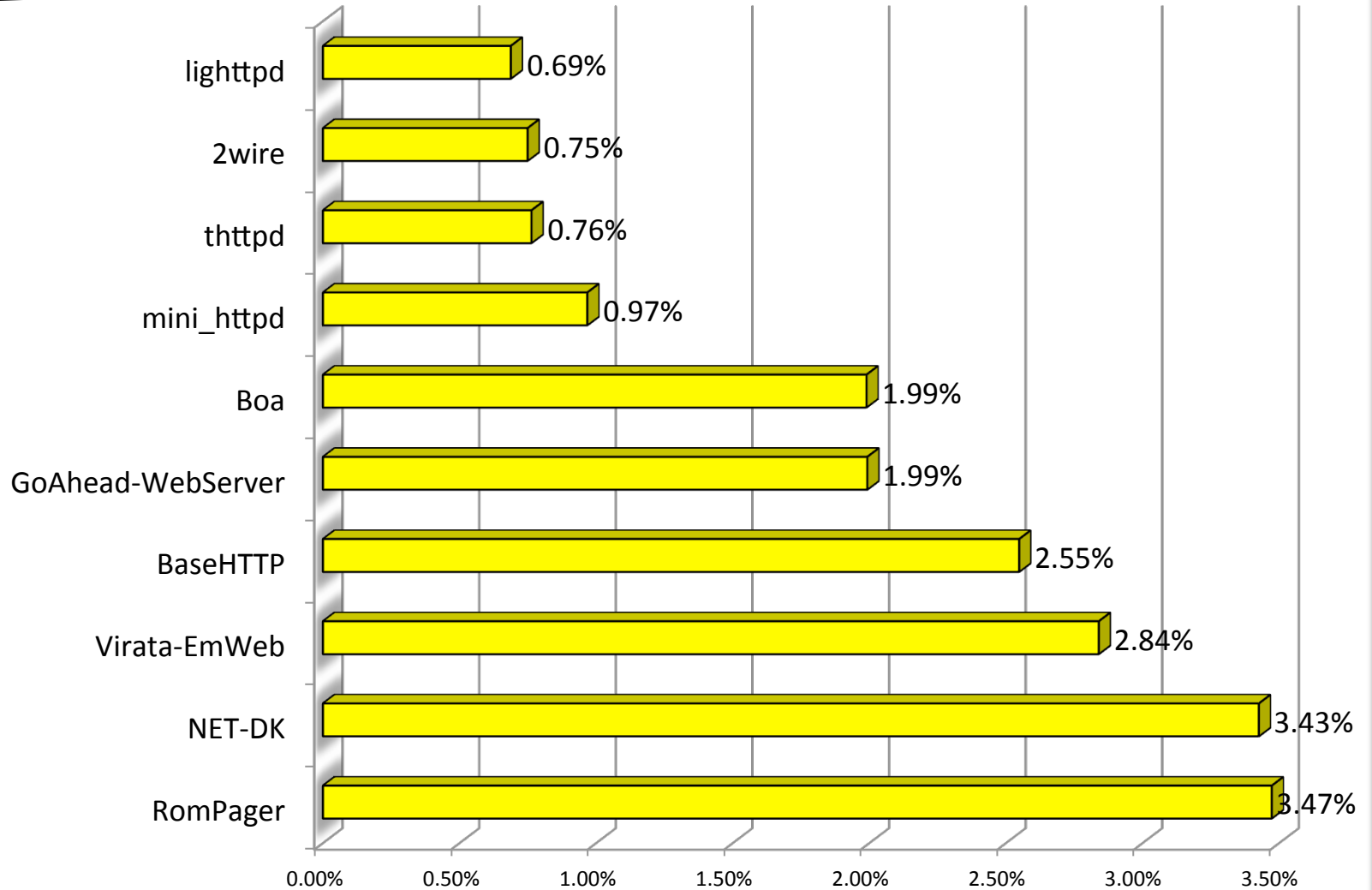
...but what the heck are these?

We know what these web servers are...

- 2,737 unique server headers identified



Top 10 EWSs



EWS Vulnerabilities

Vulnerability	CVE/BID	Vuln. Ver	Shodan
Virata-EmWeb			
URI Remote DoS	39257	6.0.1	104,919
Unauthorized DSL Modem Access	CVE-2006-0248	6.1.0	19,905
Allegro RomPager			
UPnP HTTP Request Remote DoS	45309	4.07	3,735,427

- Millions of Internet accessible devices are in use today running EWSs with known vulnerability
- Most devices have never had a firmware upgrade
- Some cannot be upgraded
- ...and this is an area of research that has been largely ignored



XSS - Xerox

The screenshot displays the Xerox CentreWare Internet Services interface for a Phaser 6200 printer. The page title is "Phaser 6200" and the status is "MPT Is Empty". A modal dialog box is overlaid on the page, displaying the URL "http://137.229.37.132" and the message "I love XSS!". The printer's status is "Error".

Xerox CentreWare Internet Services
Phaser 6200

Name: ececolor
DNS: DUCK-205-X6200-1.printers.uaf.edu
IP: 137.229.37.132

Support
Software Links
[Printer Drivers](#)
[Other Printer Software](#)

Support
http://137.229.37.132
I love XSS!

Name: ececolor
DNS: DUCK-205-X6200-1.printers.uaf.edu
IP: 137.229.37.132
Contact:
Location:
Status: Error

Refresh Status

XSS - Tektronix

Tektronix

PhaserLink™ Software for the Phaser® 850 Color Printer

[Status](#)

[Settings](#)

[More Printers](#)

[Help](#)

Startup Page

*Enabled

PhaserLink Status Refresh Delay

*60 seconds

Front Panel Menus

*Enabled

System Start Job

*Enabled

Driver settings

These settings are overridden by Tektronix drivers. If you are not using Tektronix drivers, make these settings on this page.

PhaserLink™ Software for the Phaser® 850 Color Printer

[Status](#)

[Settings](#)

[More Printers](#)

[Help](#)

Status for Phaser 850DX

Ready



http://64.131.31.50

I love XSS!

OK

PAPER TRAY(S)

Upper Tray
Letter, Paper

Lower Tray
Letter, Paper

Maintenance Kit Remaining Life
6575 Pages

LOCAL PRINTER INFORMATION

PAGE COUNT

Contact



Vendor Solutions

Functionality

- Some functionality does not offer adequate value to justify the security risk

Password protection

- Risky admin functionality should not be enabled by default
- If enabled, it should be password protected with a unique password (i.e. serial number or MAC address)

Future Proofing

- EWSs should have a user-friendly, firmware update capability



Enterprise Solutions

Preventive

- Any network enabled device should be subjected to the same security processes as a computer
- Hardening – Password protection, disabling unneeded features, firmware upgrades, etc.

Detective

- Internal/external pen tests should include EWSs
- Traditional scanning tools may (i.e. nmap) may not be appropriate



Patch Management for EWS

Frequency

- When did you last patch/scan your photocopier?

Mechanism

- Does the EWS even have a mechanism for a firmware update?

Expertise

- Traditional security scanners are unlikely to uncover/reveal vulnerable EWSs
- Manual effort will be required
- Look at both external and internal threats



Outdated EWSs – Allegro RomPager

*“In **December 1997**, Allegro delivered several additions to its embedded Internet applications product line. These included **version 2.0** of RomPager...”*

*“In **March 1999**, Allegro announced **version 3.0** of the product line...”*

*“In **April 2007**, Allegro released **version 4.6** of the RomPager family...”*

Version	Shodan
2.00	3,835
2.10	18,481
3.02	1,665
3.03	3,754
3.10	19,341
3.12	6,514
4.01	11,456
4.03	160,807
4.05	530
4.06	8089
4.10	1960
4.30	12601
4.32	1114
4.34	9910
4.61	3078





...and I am outta here!

Michael Sutton
VP, Security Research
msutton@zscaler.com
<http://research.zscaler.com>

