Open Source INTelligence (OSINT) Report for Dillard's

OSINT Executive Summary

Open Source Intelligence (OSINT) model is a collection of publicly available sources of information on a target. Information of interest includes hardware and software capacities, available employee data and points of contact, published or leaked financial information, and easily identifiable potential attack vectors.

This OSINT report is being performed for the Pentest Cantidate Program from Strategic Security. The goals of this report are:

- Amass information on Dillard.com from publically available sources, using openly available tools. Information which potentially could be used to compromise the companies network
- Identify any personal from the company along with points of contact that could be leverage in social engineering.
- Analyze available financial data and logistical data.
- Attempt to leave as little identifiable footprint while obtaining data set.

The company chosen for this report was not selected on 'good' or 'bad' merits, furthermore the information compiled is not meant to embarrass the selected company.

Dillard's Overview

Dillard's, Inc. is an upscale department store chain in the United States, with 299 stores in 28 states. Founded in 1938 by William T. Dillard; its corporate headquarters remain located in the eastern edge of Little Rock's Riverdale area.

Dillard's, Inc. operates retail department stores located primarily in the southwestern United States, offering name-brand and private-label merchandise. These brands are tantamount to Dillard's marketing strategy to drive higher profit margins, so Dillard's is introducing new lines to grow the penetration of these private label products.

Dillard's operates mall-based department stores and an e-commerce site in the United States. Primary products are sorted in the following categories:

Cosmetics (15% of net sales)
Ladies' apparel and accessories (36% of net sales)
Juniors' and children's apparel (8% of net sales)
Men's apparel and accessories (17% of net sales)
Shoes (14% of net sales)
Home and furniture (7% of net sales)

NYSE - DDS

Dec 12 12:35 PM ET
Price : 115.77
52wk Range - :82.75-125.17

COMPANY INFORMATION

1600 Cantrell Road
Little Rock, AR 72201
Post Office Box 486
(501)376-5200
(501) 376-5917 (fax)

PRODUCTS

Clothing, footwear, bedding, furniture, jewelry, beauty products, and housewares.

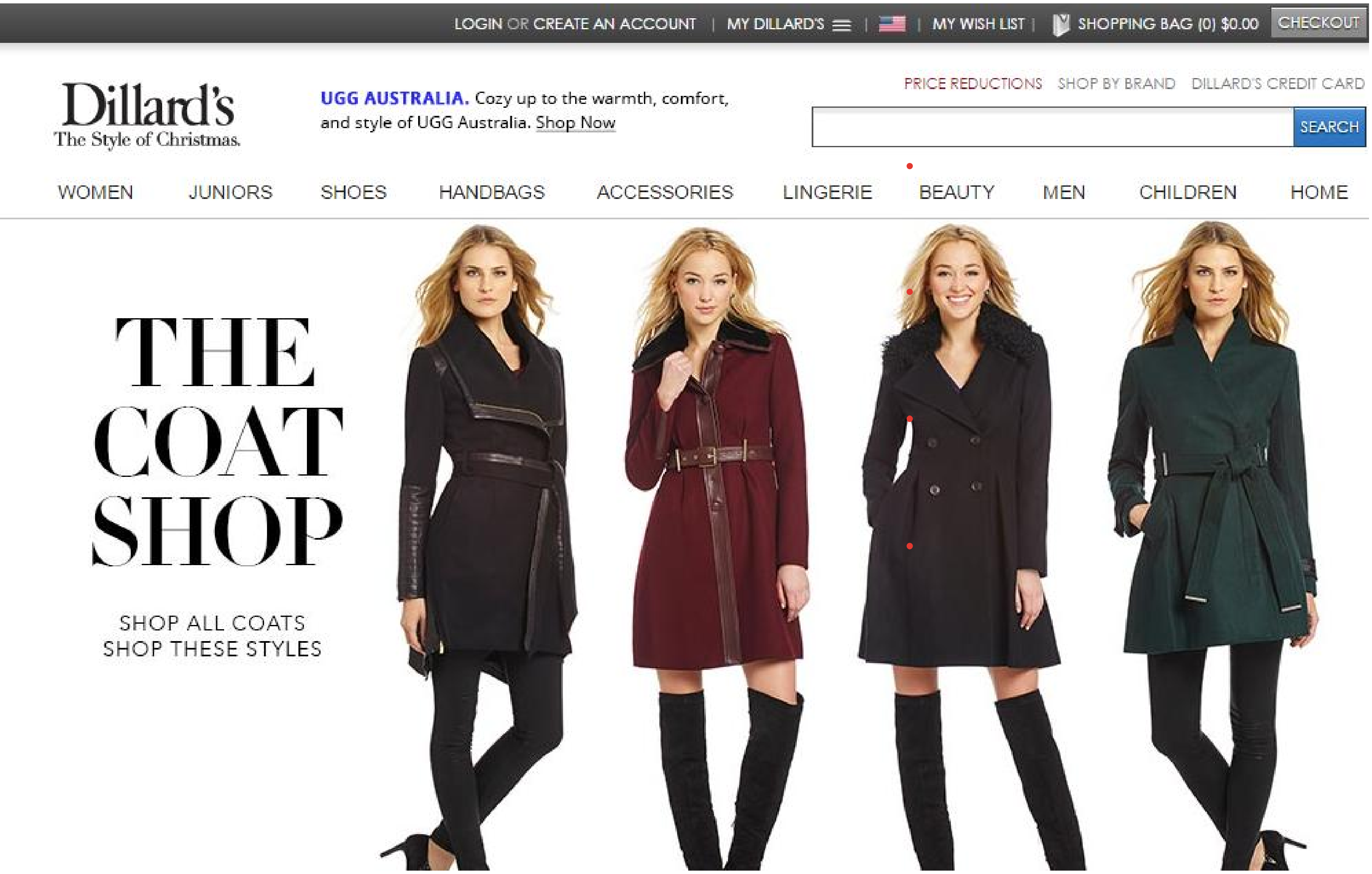
BRANDS

Chanel, Clinique, DKNY, Dior, Dolce & Gabbana, Jones New York, Levi's, and Ralph Lauren.

WEB OPERATIONS

Contact: Debbie McMahon
Phone: (501)376-5010
Fax: (501)210-9732
Public Phone: (800)643-8274

Website Home Page



UGG AUSTRALIA. Cozy up to the warmth, comfort, and style of UGG Australia. Shop Now

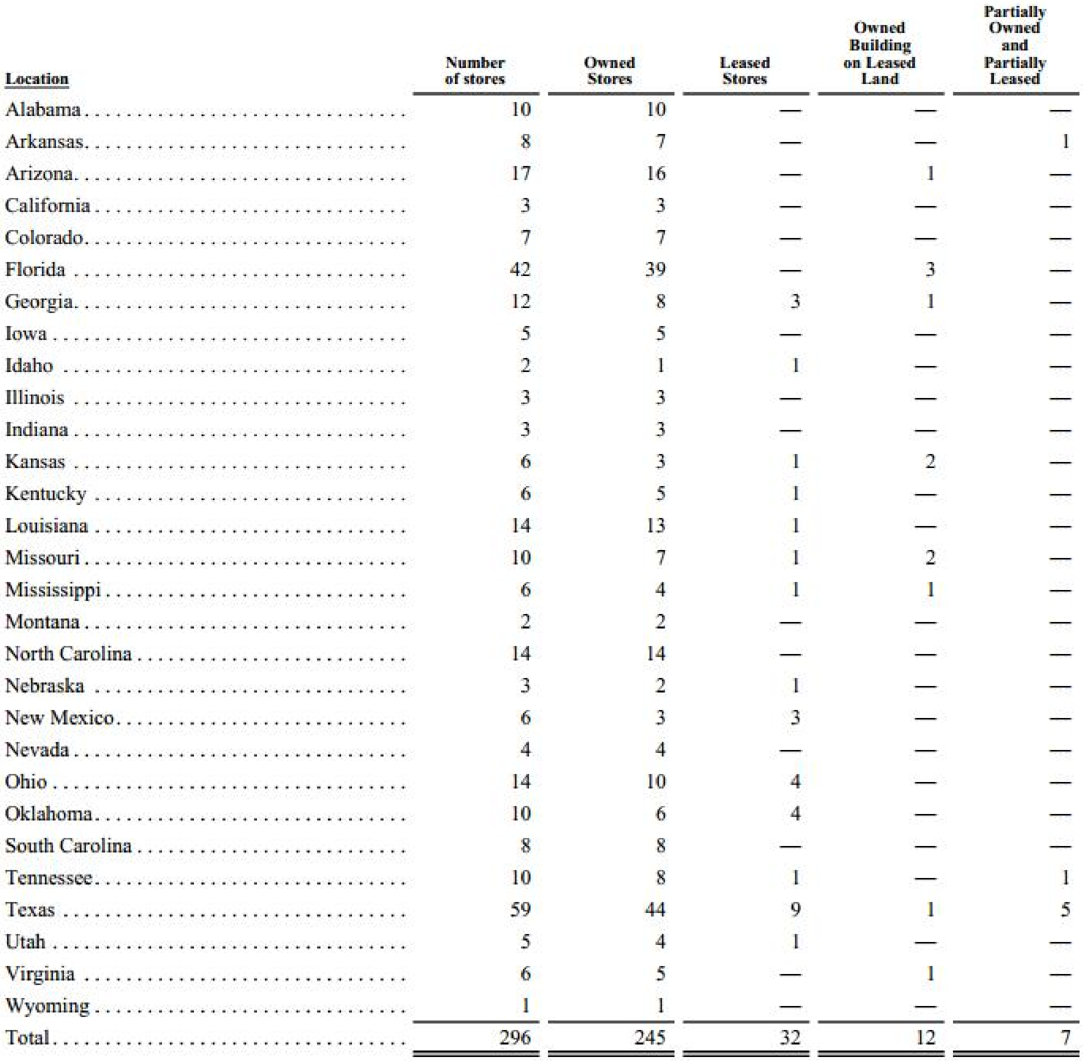
http://www.dillards.com/

Dillard’s Properties

Locations

All of Dillard’s stores are owned by the company or leased from third parties. Currently there are 296 stores in 29 states. Third-party store leases allow for rental payments based on a percentage of net sales with a guaranteed minimum annual rent.

Corporate Headquarters
Dillard's, Inc.
1600 Cantrell Rd
Little Rock, AR 72201
Phone Number: (501) 376-5200
Fax Number: (501) 376-5917



Location	Number of stores	Owned Stores	Leased Stores	Owned Building on Leased Land	Partially Owned and Partially Leased
Alabama	10	10	—	—	—
Arkansas	8	7	—	—	1
Arizona	17	16	—	1	—
California	3	3	—	—	—
Colorado	7	7	—	—	—
Florida	42	39	—	3	—
Georgia	12	8	3	1	—
Iowa	5	5	—	—	—
Idaho	2	1	1	—	—
Illinois	3	3	—	—	—
Indiana	3	3	—	—	—
Kansas	6	3	1	2	—
Kentucky	6	5	1	—	—
Louisiana	14	13	1	—	—
Missouri	10	7	1	2	—
Mississippi	6	4	1	1	—
Montana	2	2	—	—	—
North Carolina	14	14	—	—	—
Nebraska	3	2	1	—	—
New Mexico	6	3	3	—	—
Nevada	4	4	—	—	—
Ohio	14	10	4	—	—
Oklahoma	10	6	4	—	—
South Carolina	8	8	—	—	—
Tennessee	10	8	1	—	1
Texas	59	44	9	1	5
Utah	5	4	1	—	—
Virginia	6	5	—	1	—
Wyoming	1	1	—	—	—
Total	296	245	32	12	7

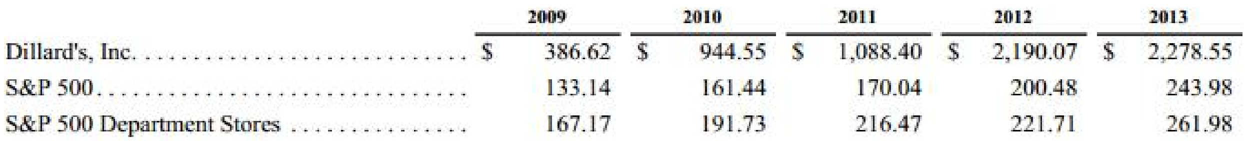
List of store locations taken from 2013 Dillard’s Annual Report (Table 1)

Dillard’s Stock Proformance

(DDS) Stock History

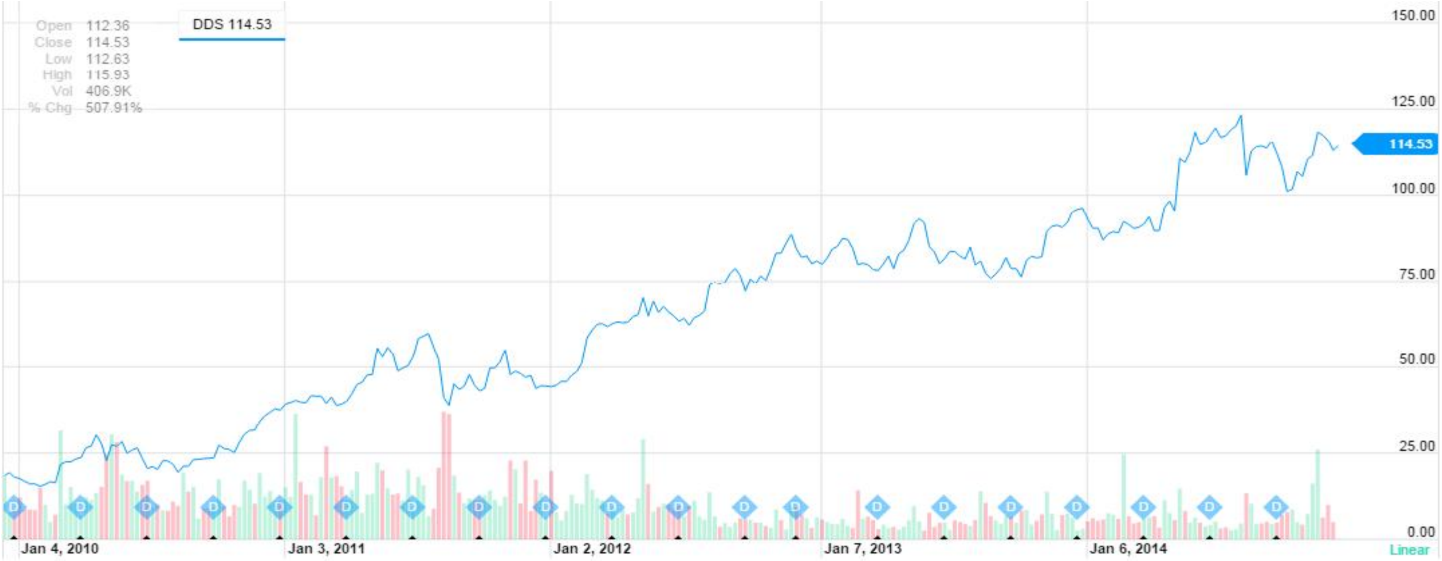
As of March 1, 2014, there were 3,130 holders of record of the Company's Class A Common Stock and 8 holders of record of the Company's Class B Common Stock. Dividends per share have remained constant at $.05 for the past two years , except for the third and fourth quarter of 2013 when dividends rose to $.06 per share.

The DDS stock on the NYSE has shown steady performance in the last four years, going from $22 in Jan 2010 to $114 in Dec 2014.



	2009	2010	2011	2012	2013
Dillard's, Inc.	$ 386.62	$ 944.55	$ 1,088.40	$ 2,190.07	$ 2,278.55
S&P 500	133.14	161.44	170.04	200.48	243.98
S&P 500 Department Stores	167.17	191.73	216.47	221.71	261.98

Shows the dollar value of $100 investments for the last five years. Take from 2013 Dillard’s Annual Report (Table 2).



Four year history on Dillard’s (DDS) Stock provided by Yahoo Finance

Dillard’s Financial Proformance

Financial Overview

(As of Dec 31, 2013)

Company financial performance in 2013

Net sales	$ 6,531,647
Cost of sales	$ 4,223,715
Gross profit from net sales	35.3%
Net income	323,671
Number of stores opened	0
Number of stores closed	6
Total stockholders’ equity	$1,992,197
Total Assets	$4,459,915
Total current assets	$ 2,037,544

(As of Nov 1, 2014)

Preliminary financial performance up to Nov 1, 2014

Net sales	$ 4,485,579
Cost of sales	$ 2,839,936
Total stockholders’ equity	$1,992,197
Total Assets	$4,459,915
Total current assets	$ 2,037,544
Net income	$201,363

Recent Performance

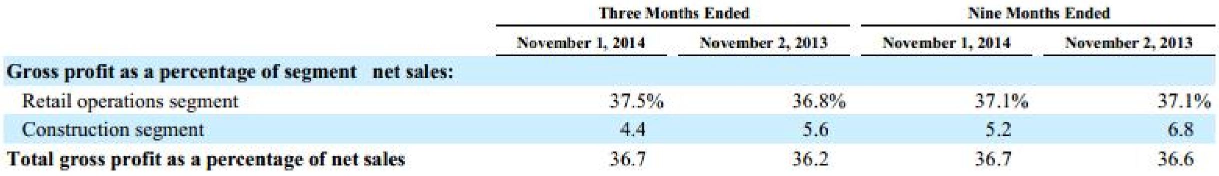
During the quarter ended November 1, 2014, comparable store sales declined 1% over last year's third quarter. Weaker sales contributed to a 70 basis points of sales increase in expenses. Gross margin from retail operations improved 69 basis points of sales. Net income increased to $55.2 million for the current year third quarter from $50.9 million for the prior year third quarter. Earnings have risen per share to $1.30 per share from $1.13 per share, a 15% increase over last year's third quarter.

Gross Profit

Gross profit of net sales improved to $535,338 at the end of November 1, 2014 compared to the $531,205 at the end November 2, 2013.

Financial Condition

In April 2014, the Company announced that it entered into a 10-year agreement with Wells Fargo Bank, N.A. ("Wells Fargo"), which took effect in November 2014. While the future of this deal is unknown, Dillard’s expects income and exclusive of startup costs from the new agreement to be comparable to the Company's historical earnings.



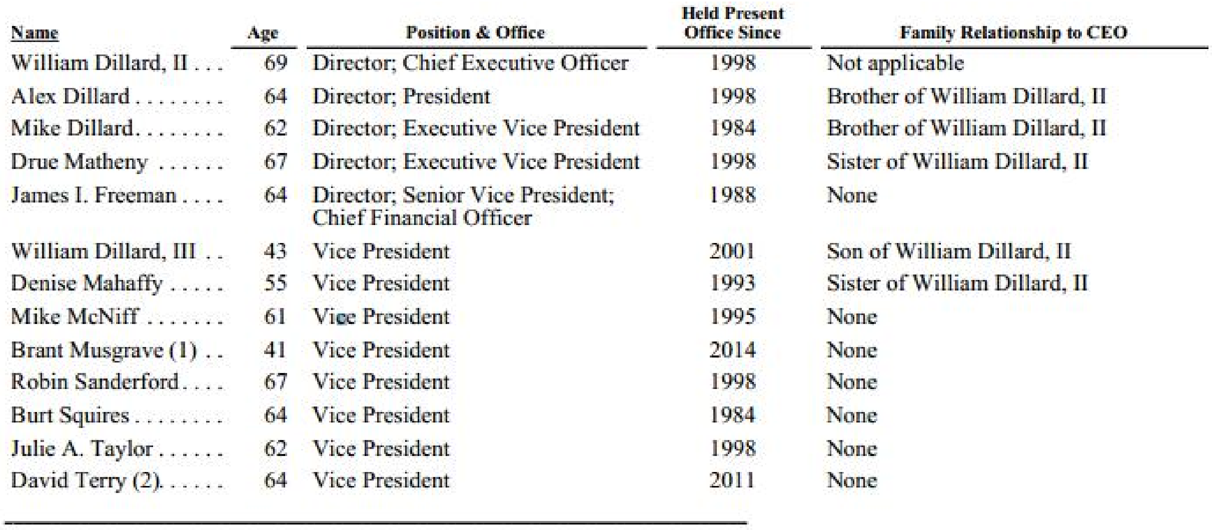
	Three Months Ended		Nine Months Ended	
	November 1, 2014	November 2, 2013	November 1, 2014	November 2, 2013
Gross profit as a percentage of segment net sales:				
Retail operations segment	37.5%	36.8%	37.1%	37.1%
Construction segment	4.4	5.6	5.2	6.8
Total gross profit as a percentage of net sales	36.7	36.2	36.7	36.6

Gross Profit in third quarter of 2014 form Dillard’s Quarterly report (Table 3)

Company Hierarchy

Executive Officers of the Registrant

Dillard's has a corporate structure with the CEO, the company's namesake, heading the organization and family members in highest positions in the organization which has a formal statement of Beneficial Ownership. Officers include four other Directors and eight Vice Presidents. The following table contains names and ages of all executive officers, including the nature of any family relationship between executives. (Each is elected to serve a one-year term.)



Name	Age	Position & Office	Held Present Office Since	Family Relationship to CEO
William Dillard, II . . .	69	Director; Chief Executive Officer	1998	Not applicable
Alex Dillard	64	Director; President	1998	Brother of William Dillard, II
Mike Dillard.	62	Director; Executive Vice President	1984	Brother of William Dillard, II
Drue Matheny	67	Director; Executive Vice President	1998	Sister of William Dillard, II
James I. Freeman	64	Director; Senior Vice President; Chief Financial Officer	1988	None
William Dillard, III . .	43	Vice President	2001	Son of William Dillard, II
Denise Mahaffy	55	Vice President	1993	Sister of William Dillard, II
Mike McNiff	61	Vice President	1995	None
Brant Musgrave (1) . .	41	Vice President	2014	None
Robin Sanderford. . . .	67	Vice President	1998	None
Burt Squires	64	Vice President	1984	None
Julie A. Taylor	62	Vice President	1998	None
David Terry (2).	64	Vice President	2011	None

(1) Mr. Musgrave served as a Regional Vice President of Stores from 2007 to 2014. In 2014, he was promoted to Corporate Vice President of Stores.

(2) Mr. Terry served as Regional President of Merchandising from 2006 to 2011. In 2011, he was promoted to Corporate Vice President of Merchandising.

Table Taken from the Dillard's 2013 Annual Report (table 4)

Family Executive Pay Summery

- William Dillard II's base salary reached $1 million for the first time, up from $950,000 in 2012.
- Alex Dillard's base salary also went up by $50,000, to $970,000 in 2013.
- Mike Dillard got a raise of $20,000, to $695,000, in his base salary.
- Matheny Dillard's base salary went from $675,000 to $695,000.
- James Freeman, the only non-family member among the named executive officers, earned a salary of $750,000 — up by $40,000 from 2012.
- Denise Mahaffy, sister of William, Alex, Mike and Drue, was paid a salary and bonus of $700,000 as a vice president of the company.
- William Dillard III, son of the CEO, was paid $725,000 in salary and bonus, plus $73,016 in benefits.
- Alexandra Dillard, daughter of Alex Dillard, was paid $227,500 in salary and bonus as a divisional merchandise manager.
- Annemarie Dillard, another daughter of Alex Dillard, was paid $180,000 as a manager.

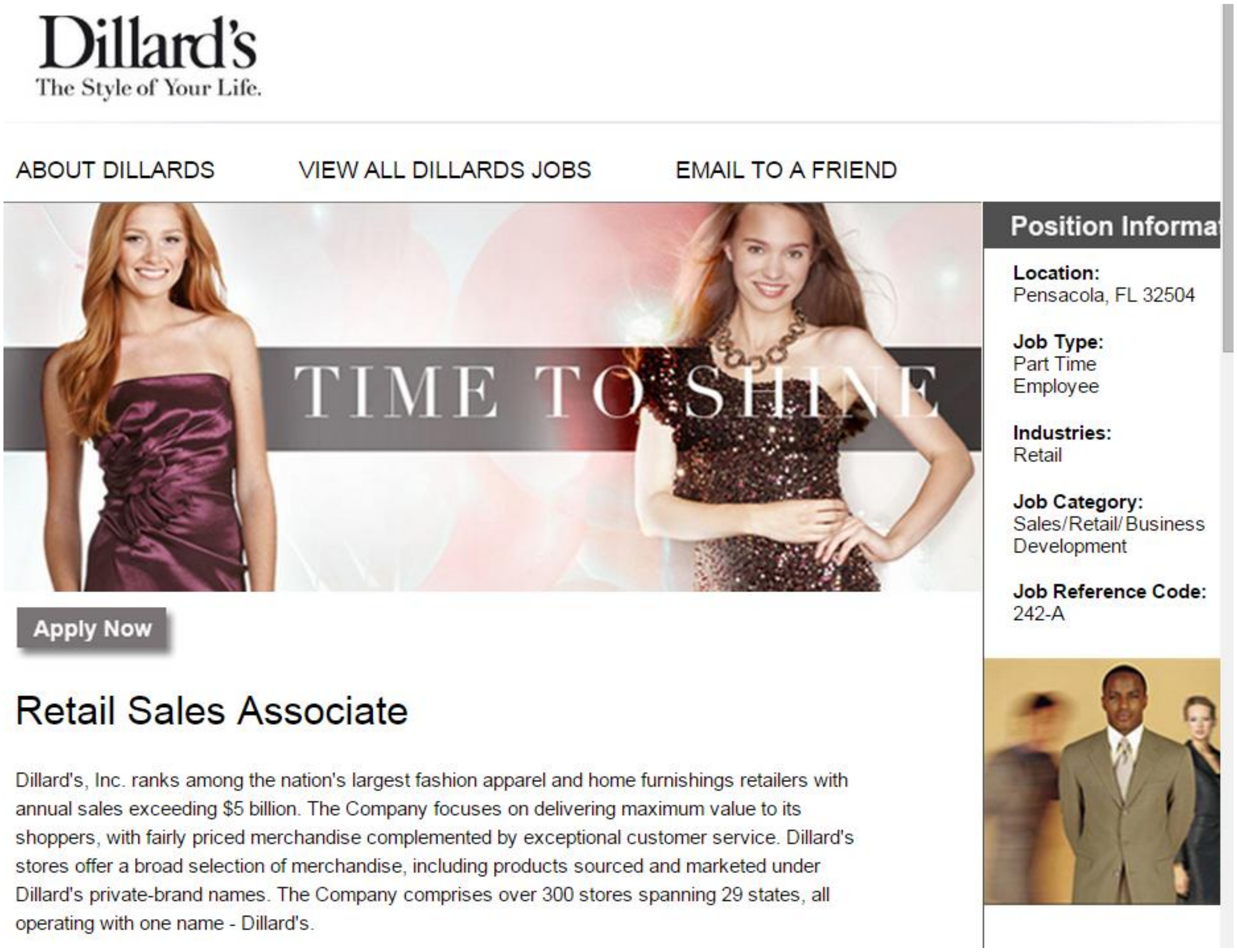
Information obtained from Dillard's Proxy Report 2013

Employment Opportunities

Job Listings

There are 350 unique job listings by Dillard on Moster.com. The most common listing is the 'Retail Sales Associate' (300/ 350 listings) position, other notables include; 'Dillard's Licensed Cosmetologist' and 'Dillard's Sales Manager'.

Retail Sales Associate



Location:
Pensacola, FL 32504

Job Type:
Part Time
Employee

Industries:
Retail

Job Category:
Sales/Retail/ Business
Development

Job Reference Code:
242-A

Retail Sales Associate

Dillard's, Inc. ranks among the nation's largest fashion apparel and home furnishings retailers with annual sales exceeding $5 billion. The Company focuses on delivering maximum value to its shoppers, with fairly priced merchandise complemented by exceptional customer service. Dillard's stores offer a broad selection of merchandise, including products sourced and marketed under Dillard's private-brand names. The Company comprises over 300 stores spanning 29 states, all operating with one name - Dillard's.

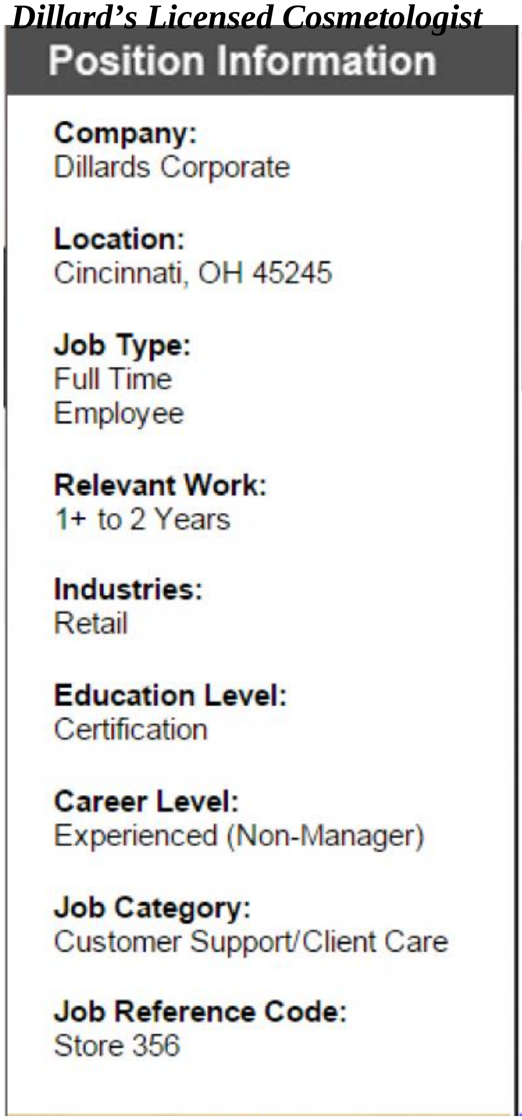
Employment Opportunities

Job Listing (cont)

Benefits

- Generous employee discount
- Exciting work environment
- Healthcare plan
- Dental/Vision
- Paid vacation
- Retirement plan

Dillard's Licensed Cosmetologist



Position Information

Company:
Dillards Corporate

Location:
Cincinnati, OH 45245

Job Type:
Full Time
Employee

Relevant Work:
1+ to 2 Years

Industries:
Retail

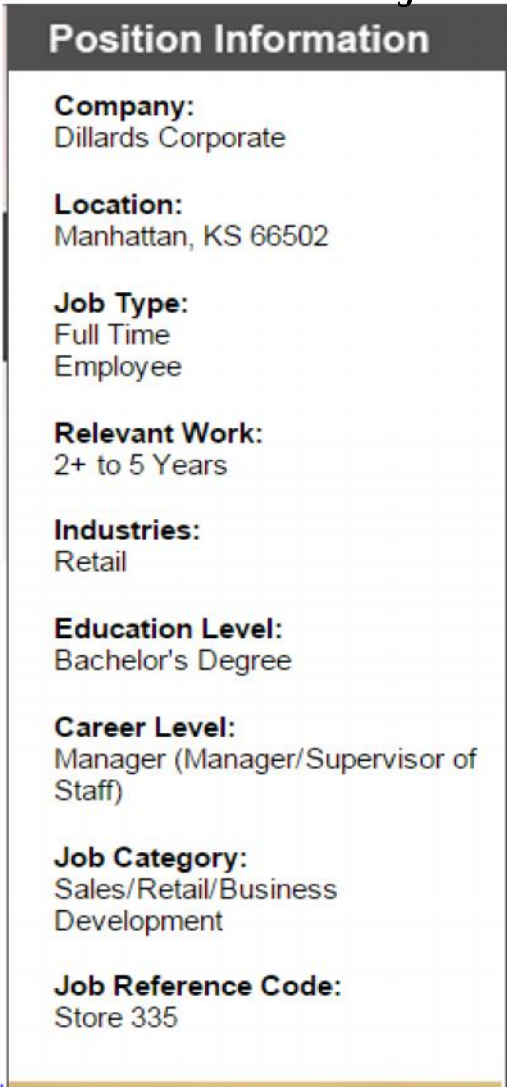
Education Level:
Certification

Career Level:
Experienced (Non-Manager)

Job Category:
Customer Support/Client Care

Job Reference Code:
Store 356

Dillard's Sales Manager



Position Information

Company:
Dillards Corporate

Location:
Manhattan, KS 66502

Job Type:
Full Time
Employee

Relevant Work:
2+ to 5 Years

Industries:
Retail

Education Level:
Bachelor's Degree

Career Level:
Manager (Manager/Supervisor of Staff)

Job Category:
Sales/Retail/Business Development

Job Reference Code:
Store 335

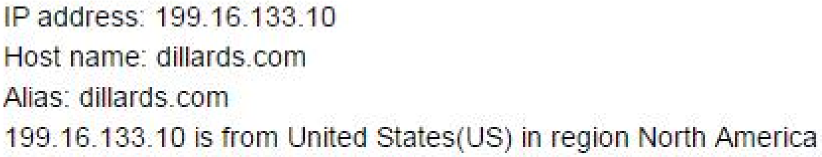
Infrastructure Identification

Infrastructure Footprint

An organization with any magnitude will have infrastructure to support their online enterprising and manage logistics. An infrastructure footprint looks to identify connected systems controlled by an organization.

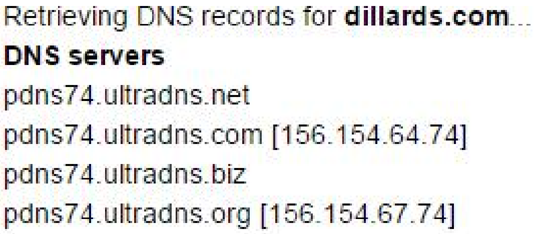
Goals

- Locate Dillard's servers and other connected equipment.
- Identify the technology used by the company



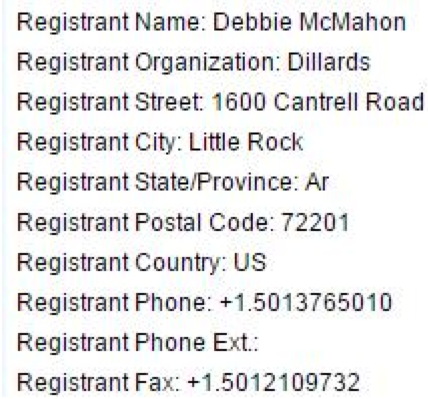
```
IP address: 199.16.133.10
Host name: dillards.com
Alias: dillards.com
199.16.133.10 is from United States(US) in region North America
```

Website IP address



```
Retrieving DNS records for dillards.com...
DNS servers
pdns74.ultradns.net
pdns74.ultradns.com [156.154.64.74]
pdns74.ultradns.biz
pdns74.ultradns.org [156.154.67.74]
```

Four name servers



```
Registrant Name: Debbie McMahon
Registrant Organization: Dillards
Registrant Street: 1600 Cantrell Road
Registrant City: Little Rock
Registrant State/Province: Ar
Registrant Postal Code: 72201
Registrant Country: US
Registrant Phone: +1.5013765010
Registrant Phone Ext.:
Registrant Fax: +1.5012109732
```

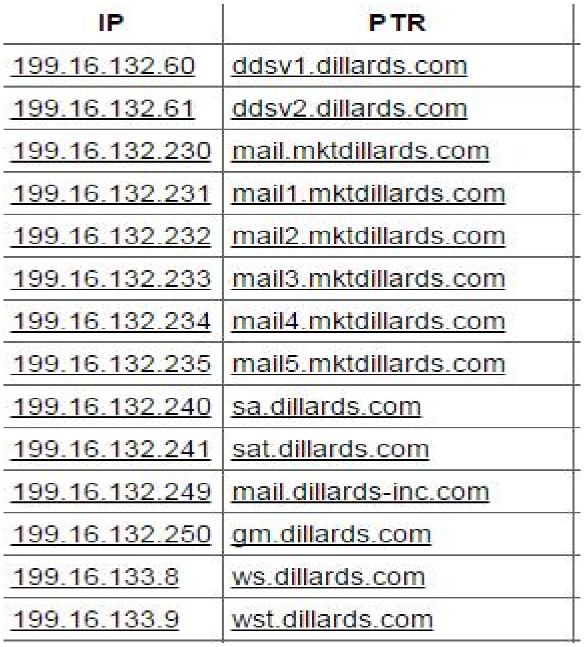
Technical person of contact

Infrastructure Identification

Mail Servers

segd.dillards.com	No A Record (no glue either)
domino2.dillards.com	199.16.135.248
domino1.dillards.com	199.16.135.248
domino.dillards.com	199.16.135.248
sysw3.dillards.com	No A Record (no glue either)
mail.dillards.com	199.16.132.249
dillards.com.s8b2.psmtp.com	64.18.7.14 (no glue)
dillards.com.s8b1.psmtp.com	64.18.7.13 (no glue)
dillards.com.s8a2.psmtp.com	64.18.7.11 (no glue)
dillards.com.s8a1.psmtp.com	64.18.7.10 (no glue)

Mail Servers (cont)



IP	PTR
199.16.132.60	ddsv1.dillards.com
199.16.132.61	ddsv2.dillards.com
199.16.132.230	mail.mktdillards.com
199.16.132.231	mail1.mktdillards.com
199.16.132.232	mail2.mktdillards.com
199.16.132.233	mail3.mktdillards.com
199.16.132.234	mail4.mktdillards.com
199.16.132.235	mail5.mktdillards.com
199.16.132.240	sa.dillards.com
199.16.132.241	sat.dillards.com
199.16.132.249	mail.dillards-inc.com
199.16.132.250	gm.dillards.com
199.16.133.8	ws.dillards.com
199.16.133.9	wst.dillards.com

Source: bgp.he.net – Table 5

DNS Records (excluding Mail and Name Servers)

Name	Class	Type	Data
dillards.com	IN	A	199.16.133.10
dillards.com	IN	SOA	pdns74.ultradns.com
dillards.com	IN	TXT	v=spf1 ip4:199.16.132.249 ip4:199.16.132.250 include:_spf.google.com ~all
10.133.16.199.in-addr.arpa	IN	PTR	origin.www.dillards.com
133.16.199.in-addr.arpa	IN	PTR	community.dillards.com
133.16.199.in-addr.arpa	IN	SOA	server: pdns74.ultradns.com
133.16.199.in-addr.arpa	IN	RRSIG	algorithm: RSA/SHA-1 signer's name: 199.in-addr.arpa
133.16.199.in-addr.arpa	IN	NSEC	134.16.199.in-addr.arpa

Network Address Lookup

NetRange:	199.16.132.0 - 199.16.135.255
CIDR:	199.16.132.0/22
Primary Server location:	Little Rock, Arkansas
Creation Date:	19-apr-1995
Expiration Date:	20-apr-2017

DNS Brute Force Results

```
www.dillards.com:23.0.28.228
www1.dillards.com:92.242.144.50
www2.dillards.com:92.242.144.50
www3.dillards.com:92.242.144.50
www4.dillards.com:92.242.144.50
www5.dillards.com:92.242.144.50
ftp.dillards.com:92.242.144.50
ftp1.dillards.com:92.242.144.50
ftp2.dillards.com:92.242.144.50
ftp3.dillards.com:92.242.144.50
ftp4.dillards.com:92.242.144.50
ftp5.dillards.com:92.242.144.50
web.dillards.com:92.242.144.50
web1.dillards.com:92.242.144.50
web2.dillards.com:92.242.144.50
web3.dillards.com:92.242.144.50
web4.dillards.com:92.242.144.50
web5.dillards.com:92.242.144.50
upload.dillards.com:92.242.144.50
upload1.dillards.com:92.242.144.50
upload2.dillards.com:92.242.144.50
upload3.dillards.com:92.242.144.50
upload4.dillards.com:92.242.144.50
upload5.dillards.com:92.242.144.50
file.dillards.com:92.242.144.50
file1.dillards.com:92.242.144.50
file2.dillards.com:92.242.144.50
file3.dillards.com:92.242.144.50
file4.dillards.com:92.242.144.50
file5.dillards.com:92.242.144.50
fileserver.dillards.com:92.242.144.50
fileserver1.dillards.com:92.242.144.50
fileserver2.dillards.com:92.242.144.50
fileserver3.dillards.com:92.242.144.50
fileserver4.dillards.com:92.242.144.50
fileserver5.dillards.com:92.242.144.50
storage.dillards.com:92.242.144.50
storage1.dillards.com:92.242.144.50
storage2.dillards.com:92.242.144.50
storage3.dillards.com:92.242.144.50
storage4.dillards.com:92.242.144.50
storage5.dillards.com:92.242.144.50
backup.dillards.com:92.242.144.50
backup1.dillards.com:92.242.144.50
backup2.dillards.com:92.242.144.50
backup3.dillards.com:92.242.144.50
backup4.dillards.com:92.242.144.50
backup5.dillards.com:92.242.144.50
share.dillards.com:92.242.144.50
share1.dillards.com:92.242.144.50
share2.dillards.com:92.242.144.50
share3.dillards.com:92.242.144.50
share4.dillards.com:92.242.144.50
share5.dillards.com:92.242.144.50
router.dillards.com:92.242.144.50
router1.dillards.com:92.242.144.50
router2.dillards.com:92.242.144.50
router3.dillards.com:92.242.144.50
router4.dillards.com:92.242.144.50
router5.dillards.com:92.242.144.50
core.dillards.com:92.242.144.50
core1.dillards.com:92.242.144.50
core2.dillards.com:92.242.144.50
core3.dillards.com:92.242.144.50
core4.dillards.com:92.242.144.50
core5.dillards.com:92.242.144.50
gw.dillards.com:92.242.144.50
gw1.dillards.com:92.242.144.50
gw2.dillards.com:92.242.144.50
gw3.dillards.com:92.242.144.50
gw4.dillards.com:92.242.144.50
gw5.dillards.com:92.242.144.50
proxy.dillards.com:92.242.144.50
proxy1.dillards.com:92.242.144.50
proxy2.dillards.com:92.242.144.50
proxy3.dillards.com:92.242.144.50
proxy4.dillards.com:92.242.144.50
proxy5.dillards.com:92.242.144.50
wingate.dillards.com:92.242.144.50
wingate1.dillards.com:92.242.144.50
wingate2.dillards.com:92.242.144.50
wingate3.dillards.com:92.242.144.50
wingate4.dillards.com:92.242.144.50
wingate5.dillards.com:92.242.144.50
main.dillards.com:92.242.144.50
main1.dillards.com:92.242.144.50
main2.dillards.com:92.242.144.50
main3.dillards.com:92.242.144.50
main4.dillards.com:92.242.144.50
main5.dillards.com:92.242.144.50
noc.dillards.com:92.242.144.50
noc1.dillards.com:92.242.144.50
noc2.dillards.com:92.242.144.50
noc3.dillards.com:92.242.144.50
noc4.dillards.com:92.242.144.50
noc5.dillards.com:92.242.144.50
home.dillards.com:92.242.144.50
home1.dillards.com:92.242.144.50
home2.dillards.com:92.242.144.50
home3.dillards.com:92.242.144.50
home4.dillards.com:92.242.144.50
home5.dillards.com:92.242.144.50
radius.dillards.com:92.242.144.50
radius1.dillards.com:92.242.144.50
radius2.dillards.com:92.242.144.50
radius3.dillards.com:92.242.144.50
radius4.dillards.com:92.242.144.50
radius5.dillards.com:92.242.144.50
firewall.dillards.com:92.242.144.50
firewall1.dillards.com:92.242.144.50
firewall2.dillards.com:92.242.144.50
firewall3.dillards.com:92.242.144.50
firewall4.dillards.com:92.242.144.50
firewall5.dillards.com:92.242.144.50
fw.dillards.com:92.242.144.50
fw1.dillards.com:92.242.144.50
fw2.dillards.com:92.242.144.50
fw3.dillards.com:92.242.144.50
fw4.dillards.com:92.242.144.50
fw5.dillards.com:92.242.144.50
vpn.dillards.com:92.242.144.50
vpn1.dillards.com:92.242.144.50
vpn2.dillards.com:92.242.144.50
vpn3.dillards.com:92.242.144.50
vpn4.dillards.com:92.242.144.50
vpn5.dillards.com:92.242.144.50
secure.dillards.com:92.242.144.50
secure1.dillards.com:92.242.144.50
secure2.dillards.com:92.242.144.50
secure3.dillards.com:92.242.144.50
secure4.dillards.com:92.242.144.50
secure5.dillards.com:92.242.144.50
security.dillards.com:92.242.144.50
security1.dillards.com:92.242.144.50
security2.dillards.com:92.242.144.50
security3.dillards.com:92.242.144.50
security4.dillards.com:92.242.144.50
security5.dillards.com:92.242.144.50
access.dillards.com:92.242.144.50
access1.dillards.com:92.242.144.50
access2.dillards.com:92.242.144.50
access3.dillards.com:92.242.144.50
access4.dillards.com:92.242.144.50
access5.dillards.com:92.242.144.50
ids.dillards.com:92.242.144.50
ids1.dillards.com:92.242.144.50
 ids2.dillards.com:92.242.144.50
ids3.dillards.com:92.242.144.50
ids4.dillards.com:92.242.144.50
ids5.dillards.com:92.242.144.50
dmz.dillards.com:92.242.144.50
dmz1.dillards.com:92.242.144.50
dmz2.dillards.com:92.242.144.50
dmz3.dillards.com:92.242.144.50
dmz4.dillards.com:92.242.144.50
dmz5.dillards.com:92.242.144.50
ns.dillards.com:92.242.144.50
ns1.dillards.com:92.242.144.50
ns2.dillards.com:92.242.144.50
ns3.dillards.com:92.242.144.50
ns4.dillards.com:92.242.144.50
ns5.dillards.com:92.242.144.50
dns.dillards.com:92.242.144.50
dns1.dillards.com:92.242.144.50
dns2.dillards.com:92.242.144.50
dns3.dillards.com:92.242.144.50
dns4.dillards.com:92.242.144.50
dns5.dillards.com:92.242.144.50
domain.dillards.com:92.242.144.50
domain1.dillards.com:92.242.144.50
domain2.dillards.com:92.242.144.50
domain3.dillards.com:92.242.144.50
domain4.dillards.com:92.242.144.50
domain5.dillards.com:92.242.144.50
nameserver.dillards.com:92.242.144.50
nameserver1.dillards.com:92.242.144.50
nameserver2.dillards.com:92.242.144.50
nameserver3.dillards.com:92.242.144.50
nameserver4.dillards.com:92.242.144.50
nameserver5.dillards.com:92.242.144.50
sql.dillards.com:92.242.144.50
sql1.dillards.com:92.242.144.50
sql2.dillards.com:92.242.144.50
sql3.dillards.com:92.242.144.50
sql4.dillards.com:92.242.144.50
sql5.dillards.com:92.242.144.50
mysql.dillards.com:92.242.144.50
mysql1.dillards.com:92.242.144.50
mysql2.dillards.com:92.242.144.50
mysql3.dillards.com:92.242.144.50
mysql4.dillards.com:92.242.144.50
mysql5.dillards.com:92.242.144.50
mssql.dillards.com:92.242.144.50
mssql1.dillards.com:92.242.144.50
mssql2.dillards.com:92.242.144.50
mssql3.dillards.com:92.242.144.50
mssql4.dillards.com:92.242.144.50
mssql5.dillards.com:92.242.144.50
postgres.dillards.com:92.242.144.50
postgres1.dillards.com:92.242.144.50
postgres2.dillards.com:92.242.144.50
postgres3.dillards.com:92.242.144.50
postgres4.dillards.com:92.242.144.50
postgres5.dillards.com:92.242.144.50
db.dillards.com:92.242.144.50
db1.dillards.com:92.242.144.50
db2.dillards.com:92.242.144.50
db3.dillards.com:92.242.144.50
db4.dillards.com:92.242.144.50
db5.dillards.com:92.242.144.50
database.dillards.com:92.242.144.50
database1.dillards.com:92.242.144.50
database2.dillards.com:92.242.144.50
```

Infrastructure Identification

DNS Brute Force Results (cont)

```
database3.dillards.com:92.242.144.50
database4.dillards.com:92.242.144.50
database5.dillards.com:92.242.144.50
mail.dillards.com:199.16.132.249
mail1.dillards.com:92.242.144.50
mail2.dillards.com:92.242.144.50
mail3.dillards.com:92.242.144.50
mail4.dillards.com:92.242.144.50
mail5.dillards.com:92.242.144.50
imail.dillards.com:92.242.144.50
imail1.dillards.com:92.242.144.50
imail2.dillards.com:92.242.144.50
imail3.dillards.com:92.242.144.50
imail4.dillards.com:92.242.144.50
imail5.dillards.com:92.242.144.50
mx.dillards.com:92.242.144.50
mx1.dillards.com:92.242.144.50
mx2.dillards.com:92.242.144.50
mx3.dillards.com:92.242.144.50
mx4.dillards.com:92.242.144.50
mx5.dillards.com:92.242.144.50
smtp.dillards.com:92.242.144.50
smtp1.dillards.com:92.242.144.50
smtp2.dillards.com:92.242.144.50
smtp3.dillards.com:92.242.144.50
smtp4.dillards.com:92.242.144.50
smtp5.dillards.com:92.242.144.50
imap.dillards.com:92.242.144.50
imap1.dillards.com:92.242.144.50
imap2.dillards.com:92.242.144.50
imap3.dillards.com:92.242.144.50
imap4.dillards.com:92.242.144.50
imap5.dillards.com:92.242.144.50
pop.dillards.com:92.242.144.50
pop1.dillards.com:92.242.144.50
pop2.dillards.com:92.242.144.50
pop3.dillards.com:92.242.144.50
pop4.dillards.com:92.242.144.50
pop5.dillards.com:92.242.144.50
webmail.dillards.com:92.242.144.50
webmail1.dillards.com:92.242.144.50
webmail2.dillards.com:92.242.144.50
webmail3.dillards.com:92.242.144.50
webmail4.dillards.com:92.242.144.50
webmail5.dillards.com:92.242.144.50
email.dillards.com:92.242.144.50
email1.dillards.com:92.242.144.50
email2.dillards.com:92.242.144.50
email3.dillards.com:92.242.144.50
email4.dillards.com:92.242.144.50
email5.dillards.com:92.242.144.50
```

```
exchange.dillards.com:92.242.144.50
exchange1.dillards.com:92.242.144.50
exchange2.dillards.com:92.242.144.50
exchange3.dillards.com:92.242.144.50
exchange4.dillards.com:92.242.144.50
exchange5.dillards.com:92.242.144.50
sendmail.dillards.com:92.242.144.50
sendmail1.dillards.com:92.242.144.50
sendmail2.dillards.com:92.242.144.50
sendmail3.dillards.com:92.242.144.50
sendmail4.dillards.com:92.242.144.50
sendmail5.dillards.com:92.242.144.50
louts.dillards.com:92.242.144.50
louts1.dillards.com:92.242.144.50
louts2.dillards.com:92.242.144.50
louts3.dillards.com:92.242.144.50
louts4.dillards.com:92.242.144.50
louts5.dillards.com:92.242.144.50
notes.dillards.com:92.242.144.50
notes1.dillards.com:92.242.144.50
notes2.dillards.com:92.242.144.50
notes3.dillards.com:92.242.144.50
notes4.dillards.com:92.242.144.50
notes5.dillards.com:92.242.144.50
test.dillards.com:92.242.144.50
test1.dillards.com:92.242.144.50
test2.dillards.com:92.242.144.50
test3.dillards.com:92.242.144.50
test4.dillards.com:92.242.144.50
test5.dillards.com:92.242.144.50
logs.dillards.com:92.242.144.50
logs1.dillards.com:92.242.144.50
logs2.dillards.com:92.242.144.50
logs3.dillards.com:92.242.144.50
logs4.dillards.com:92.242.144.50
logs5.dillards.com:92.242.144.50
printer.dillards.com:92.242.144.50
printer1.dillards.com:92.242.144.50
printer2.dillards.com:92.242.144.50
printer3.dillards.com:92.242.144.50
printer4.dillards.com:92.242.144.50
printer5.dillards.com:92.242.144.50
stage.dillards.com:92.242.144.50
stage1.dillards.com:92.242.144.50
stage2.dillards.com:92.242.144.50
stage3.dillards.com:92.242.144.50
stage4.dillards.com:92.242.144.50
stage5.dillards.com:92.242.144.50
staging.dillards.com:92.242.144.50
staging1.dillards.com:92.242.144.50
staging2.dillards.com:92.242.144.50
staging3.dillards.com:92.242.144.50
staging4.dillards.com:92.242.144.50
staging5.dillards.com:92.242.144.50
```

```
dev.dillards.com:92.242.144.50
dev1.dillards.com:92.242.144.50
dev2.dillards.com:92.242.144.50
dev3.dillards.com:92.242.144.50
dev4.dillards.com:92.242.144.50
dev5.dillards.com:92.242.144.50
devel.dillards.com:92.242.144.50
devel1.dillards.com:92.242.144.50
devel2.dillards.com:92.242.144.50
devel3.dillards.com:92.242.144.50
devel4.dillards.com:92.242.144.50
devel5.dillards.com:92.242.144.50
ppp.dillards.com:92.242.144.50
ppp1.dillards.com:92.242.144.50
ppp2.dillards.com:92.242.144.50
ppp3.dillards.com:92.242.144.50
ppp4.dillards.com:92.242.144.50
ppp5.dillards.com:92.242.144.50
chat.dillards.com:92.242.144.50
chat1.dillards.com:92.242.144.50
chat2.dillards.com:92.242.144.50
chat3.dillards.com:92.242.144.50
chat4.dillards.com:92.242.144.50
chat5.dillards.com:92.242.144.50
irc.dillards.com:92.242.144.50
irc1.dillards.com:92.242.144.50
irc2.dillards.com:92.242.144.50
irc3.dillards.com:92.242.144.50
irc4.dillards.com:92.242.144.50
irc5.dillards.com:92.242.144.50
eng.dillards.com:92.242.144.50
eng1.dillards.com:92.242.144.50
eng2.dillards.com:92.242.144.50
eng3.dillards.com:92.242.144.50
eng4.dillards.com:92.242.144.50
eng5.dillards.com:92.242.144.50
admin.dillards.com:92.242.144.50
admin1.dillards.com:92.242.144.50
admin2.dillards.com:92.242.144.50
admin3.dillards.com:92.242.144.50
admin4.dillards.com:92.242.144.50
admin5.dillards.com:92.242.144.50
unix.dillards.com:92.242.144.50
unix1.dillards.com:92.242.144.50
unix2.dillards.com:92.242.144.50
unix3.dillards.com:92.242.144.50
unix4.dillards.com:92.242.144.50
unix5.dillards.com:92.242.144.50
linux.dillards.com:92.242.144.50
linux1.dillards.com:92.242.144.50
linux2.dillards.com:92.242.144.50
linux3.dillards.com:92.242.144.50
linux4.dillards.com:92.242.144.50
linux5.dillards.com:92.242.144.50
```

```
windows.dillards.com:92.242.144.50
windows1.dillards.com:92.242.144.50
windows2.dillards.com:92.242.144.50
windows3.dillards.com:92.242.144.50
windows4.dillards.com:92.242.144.50
windows5.dillards.com:92.242.144.50
sun.dillards.com:92.242.144.50
sun1.dillards.com:92.242.144.50
sun2.dillards.com:92.242.144.50
sun3.dillards.com:92.242.144.50
sun4.dillards.com:92.242.144.50
sun5.dillards.com:92.242.144.50
solaris.dillards.com:92.242.144.50
solaris1.dillards.com:92.242.144.50
solaris2.dillards.com:92.242.144.50
solaris3.dillards.com:92.242.144.50
solaris4.dillards.com:92.242.144.50
solaris5.dillards.com:92.242.144.50
apple.dillards.com:92.242.144.50
apple1.dillards.com:92.242.144.50
apple2.dillards.com:92.242.144.50
apple3.dillards.com:92.242.144.50
apple4.dillards.com:92.242.144.50
apple5.dillards.com:92.242.144.50
hpux.dillards.com:92.242.144.50
hpux1.dillards.com:92.242.144.50
hpux2.dillards.com:92.242.144.50
hpux3.dillards.com:92.242.144.50
hpux4.dillards.com:92.242.144.50
hpux5.dillards.com:92.242.144.50
hp-ux.dillards.com:92.242.144.50
hp-ux1.dillards.com:92.242.144.50
hp-ux2.dillards.com:92.242.144.50
database3.dillards.com:92.242.144.50
database4.dillards.com:92.242.144.50
database5.dillards.com:92.242.144.50
mail.dillards.com:199.16.132.249
mail1.dillards.com:92.242.144.50
mail2.dillards.com:92.242.144.50
mail3.dillards.com:92.242.144.50
mail4.dillards.com:92.242.144.50
mail5.dillards.com:92.242.144.50
```

Statistics

432 common c-name lookups were successful on dillards.com

List obtained using Blindcrawl

Infrastructure Identification

DNS Bruteforce Follow-up

There are two unique IP addresses provided by Blindcrawl:

- 23.0.28.228
- 92.242.144.50

IP address: **23.0.28.228**

Host name: a23-0-28-228.deploy.static.akamaitechnologies.com

23.0.28.228 is from United States

NetRange: 23.0.0.0 - 23.15.255.255

CIDR: 23.0.0.0/12

Domain Name: AKAMAITECHNOLOGIES.COM

Registrar: TUCOWS DOMAINS INC

Name Server: AX0.AKAMAISTREAM.NET

Name Server: AX1.AKAMAISTREAM.NET

Name Server: AX2.AKAMAISTREAM.NET

Name Server: AX3.AKAMAISTREAM.NET

Name Server: NS2-32.AKAMAISTREAM.NET

Name Server: NS3-32.AKAMAISTREAM.NET

Name Server: NS6-32.AKAMAISTREAM.NET

Name Server: P5.AKAMAISTREAM.NET

Name Server: P6.AKAMAISTREAM.NET

Name Server: P7.AKAMAISTREAM.NET

Name Server: P8.AKAMAISTREAM.NET

IP address: **92.242.144.50**

No host name is associated with this IP address

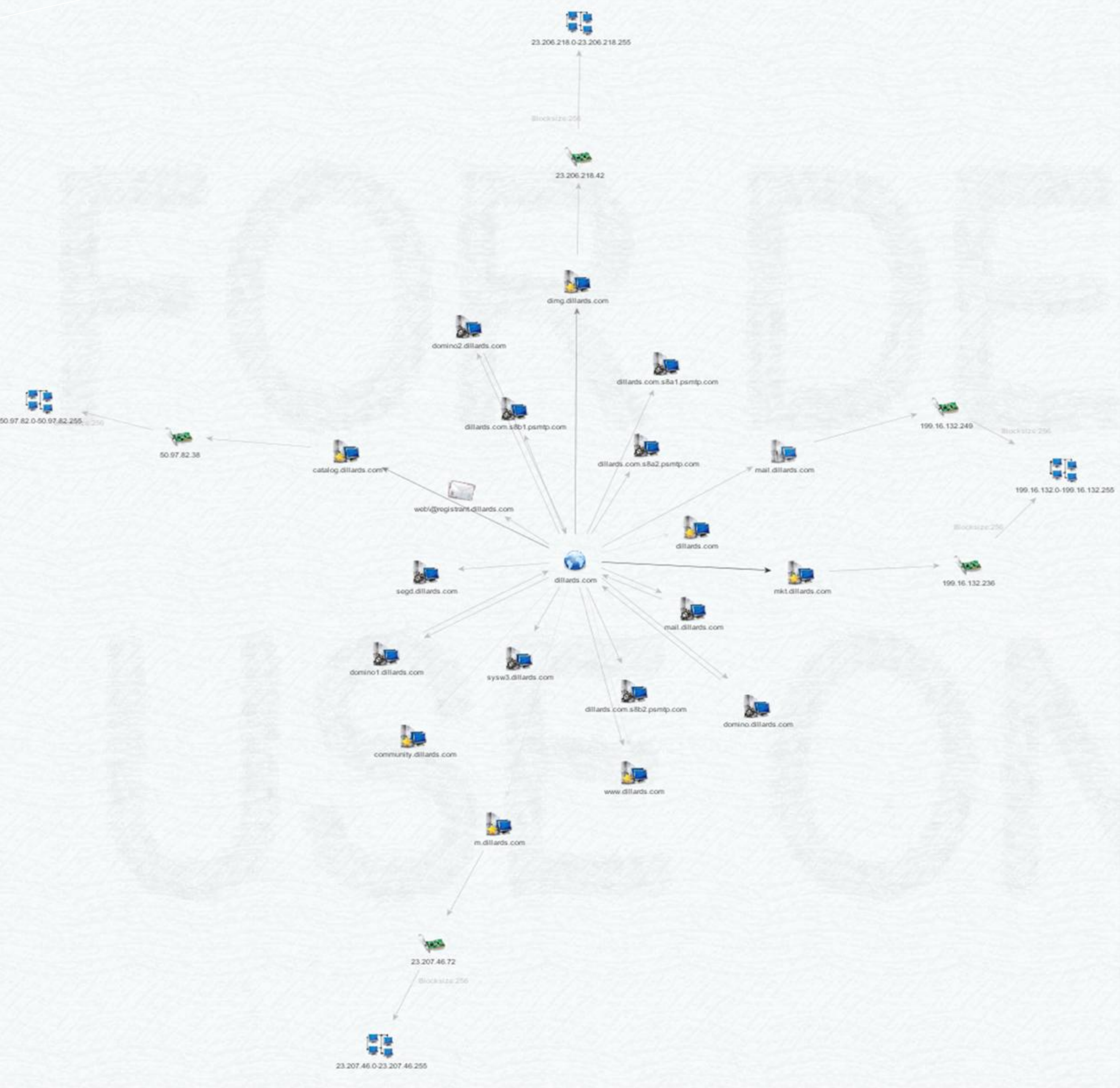
92.242.144.50 is from United Kingdom

OrgName: RIPE Network Coordination Centre

NetRange: 92.0.0.0 - 92.255.255.255

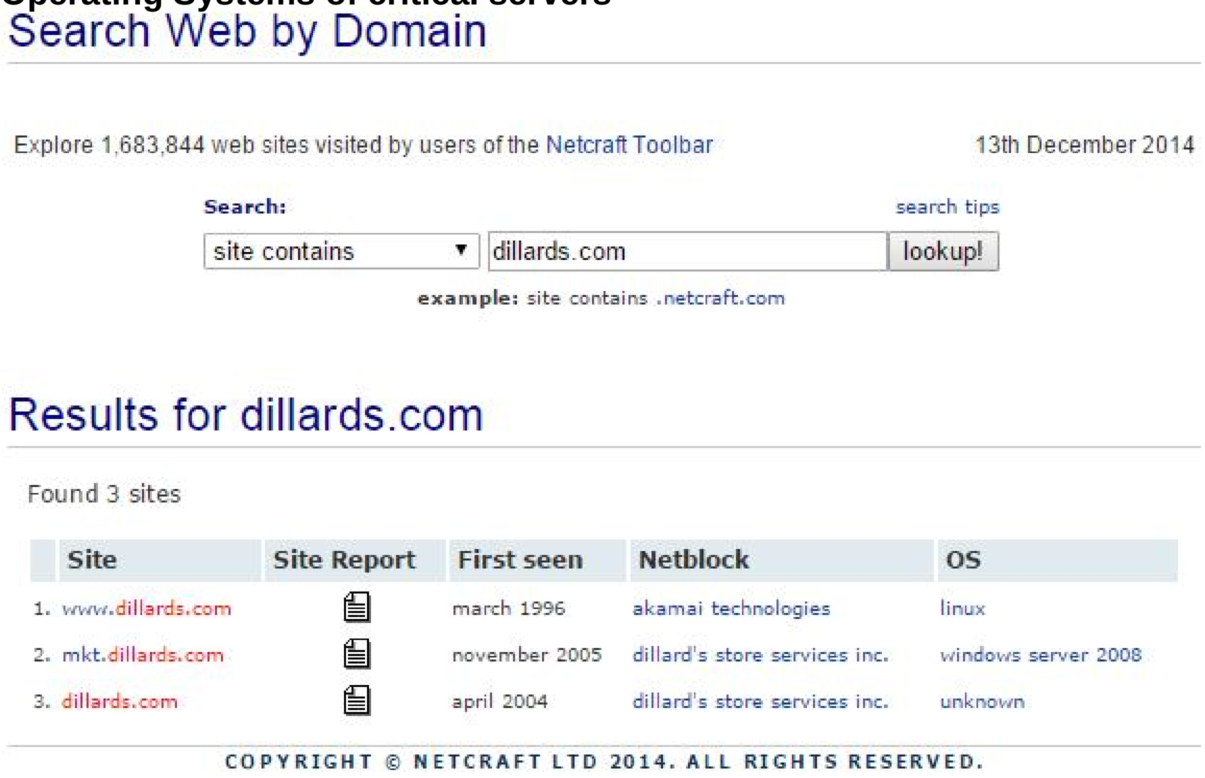
CIDR: 92.0.0.0/8

Network Diagram



Associated Infrastructure

Operating Systems of critical servers



Search Web by Domain

Explore 1,683,844 web sites visited by users of the Netcraft Toolbar 13th December 2014

Search: search tips

site contains ▼ | dillards.com | lookup!

example: site contains .netcraft.com

Results for dillards.com

Found 3 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.dillards.com	🗎	march 1996	akamai technologies	linux
2.	mkt.dillards.com	🗎	november 2005	dillard's store services inc.	windows server 2008
3.	dillards.com	🗎	april 2004	dillard's store services inc.	unknown

COPYRIGHT © NETCRAFT LTD 2014. ALL RIGHTS RESERVED.

(Source: netcraft.com – Table 6)

Follow-up Information On (mkt.dillards.com)

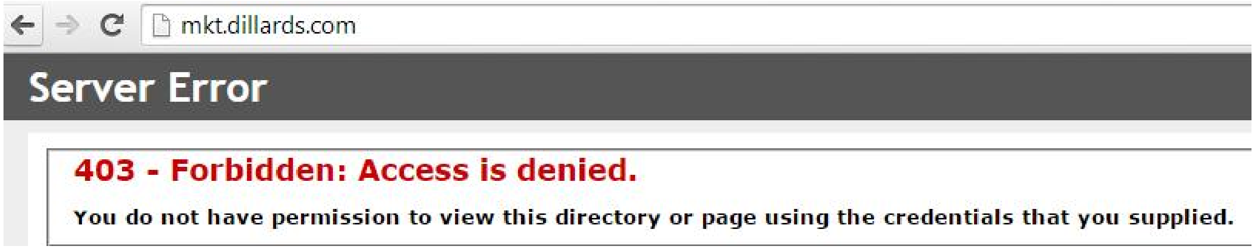
IP address: 199.16.132.236

Host name: mkt.dillards.com

Alias: mkt.dillards.com

199.16.132.236 is from United States

Answer records: mkt.dillards.com 199.16.132.236



mkt.dillards.com

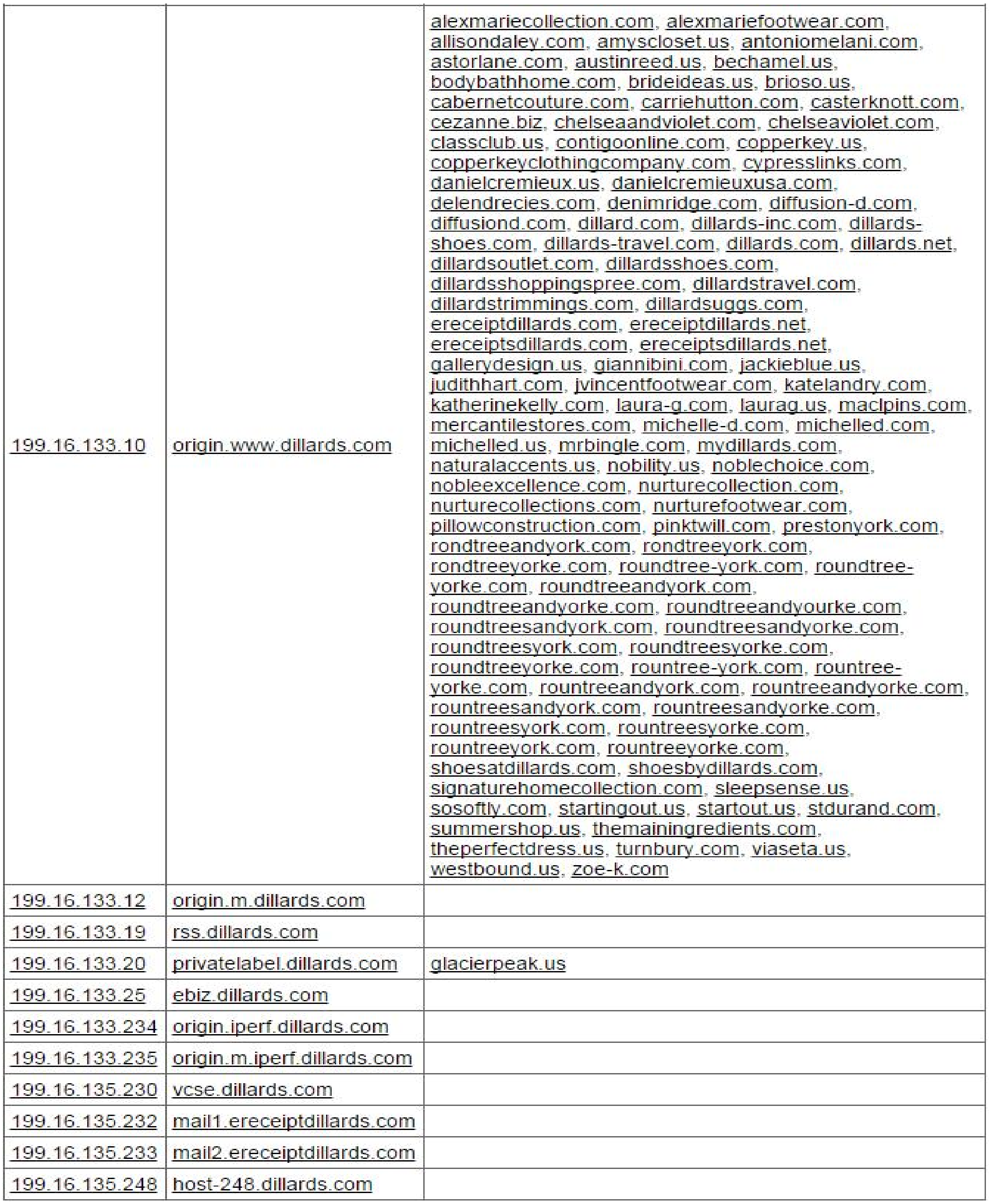
Server Error

403 - Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

Associated Web Domains

The following web addresses are under the control, falling within Dillards.com /22 IP block.



199.16.133.10	origin.www.dillards.com	alexmariecollection.com, alexmariefootwear.com, allisondaley.com, amyscloset.us, antoniomelani.com, astorlane.com, austinreed.us, bechamel.us, bodybathhome.com, brideideas.us, brioso.us, cabernetcouture.com, carriehutton.com, casterknott.com, cezanne.biz, chelseaandviolet.com, chelseaviolet.com, classclub.us, contigoonline.com, copperkey.us, copperkeyclothingcompany.com, cypresslinks.com, danielcremieux.us, danielcremieuxusa.com, delendrecies.com, denimridge.com, diffusion-d.com, diffusiond.com, dillard.com, dillards-inc.com, dillards-shoes.com, dillards-travel.com, dillards.com, dillards.net, dillardsoutlet.com, dillardsshoes.com, dillardsshoppingspree.com, dillardstravel.com, dillardstrimmings.com, dillardsuggs.com, ereceiptdillards.com, ereceiptdillards.net, ereceiptsdillards.com, ereceiptsdillards.net, gallerydesign.us, giannibini.com, jackieblue.us, judithhart.com, jvincentfootwear.com, katelandry.com, katherinekelly.com, laura-g.com, laurag.us, maclpins.com, mercantilestores.com, michelle-d.com, michelled.com, michelled.us, mrbingle.com, mydillards.com, naturalaccents.us, nobility.us, noblechoice.com, nobleexcellence.com, nurturecollection.com, nurturecollections.com, nurturefootwear.com, pillowconstruction.com, pinktwill.com, prestonyork.com, rondtreeandyork.com, rondtreeyork.com, rondtreeyorke.com, roundtree-york.com, roundtree-yorke.com, roundtreeandyork.com, roundtreeandyorke.com, roundtreeandyourke.com, roundtreesandyork.com, roundtreesandyorke.com, roundtreesyork.com, roundtreesyorke.com, roundtreeyorke.com, rountree-york.com, rountree-yorke.com, rountreeandyork.com, rountreeandyorke.com, rountreesandyork.com, rountreesandyorke.com, rountreesyork.com, rountreesyorke.com, rountreeyork.com, rountreeyorke.com, shoesatdillards.com, shoesbydillards.com, signaturehomecollection.com, sleepsense.us, sosoftly.com, startingout.us, startout.us, stdurand.com, summershop.us, themainingredients.com, theperfectdress.us, turnbury.com, viaseta.us, westbound.us, zoe-k.com
199.16.133.12	origin.m.dillards.com	
199.16.133.19	rss.dillards.com	
199.16.133.20	privatelabel.dillards.com	glacierpeak.us
199.16.133.25	ebiz.dillards.com	
199.16.133.234	origin.iperf.dillards.com	
199.16.133.235	origin.m.iperf.dillards.com	
199.16.135.230	vcse.dillards.com	
199.16.135.232	mail1.ereceiptdillards.com	
199.16.135.233	mail2.ereceiptdillards.com	
199.16.135.248	host-248.dillards.com	

Source: bgp.he.net – Table 7

Nmap List Scan

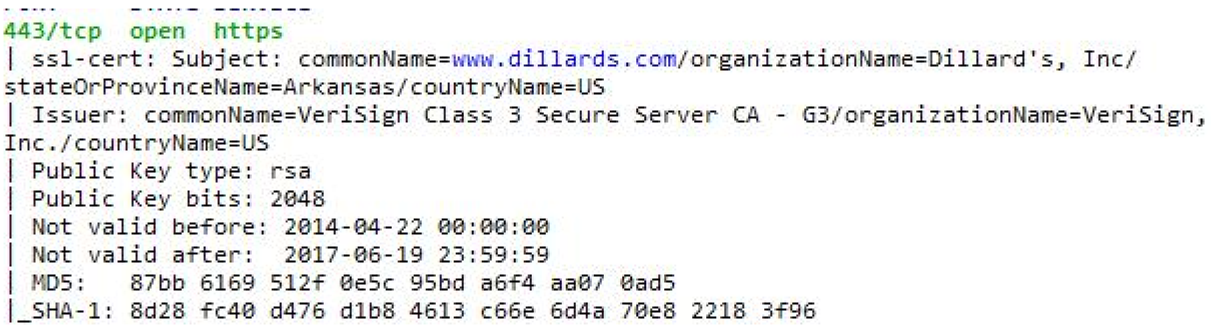
The open source port scanner Nmap was initiated using a List Scan (-sL) against Dillards IP range (199.16.132.0-199.16.135.255). The List following is all active ip address.

Nmap –sL 199.16.132.0-199.16.135.255 (Results Edited)

ddsv1.dillards.com (199.16.132.60)ddsv2.dillards.com (199.16.132.61)
mail.mktdillards.com (199.16.132.230)mail1.mktdillards.com (199.16.132.231)mail2.mktdillards.com (199.16.132.232)mail3.mktdillards.com (199.16.132.233)mail4.mktdillards.com (199.16.132.234)mail5.mktdillards.com (199.16.132.235)
sa.dillards.com (199.16.132.240)
sat.dillards.com (199.16.132.241)
mail.dillards-inc.com (199.16.132.249)
gm.dillards.com (199.16.132.250)
ws.dillards.com (199.16.133.8)
wst.dillards.com (199.16.133.9)
origin.www.dillards.com (199.16.133.10)
origin.m.dillards.com (199.16.133.12)
rss.dillards.com (199.16.133.19)
privatelabel.dillards.com (199.16.133.20)
ebiz.dillards.com (199.16.133.25)
vcse.dillards.com (199.16.135.230)
mail1.ereceiptdillards.com (199.16.135.232)
mail2.ereceiptdillards.com (199.16.135.233)
host-248.dillards.com (199.16.135.248)

Nmap -p 443,444,8443,8080,8088 --open --script ssl-cert 199.16.133.0-199.16.135.255 (Results Edited)

199.16.132.0-255 --- All ports open on up hosts (96 hosts up)
199.16.133.0-255 --- All ports open on up hosts (110 hosts up)
199.16.134.0-255 --- All ports open on up hosts (85 hosts up)
199.16.135.0-255 --- All ports open on up hosts (91 hosts up)



```
443/tcp  open  https
| ssl-cert: Subject: commonName=www.dillards.com/organizationName=Dillard's, Inc/
stateOrProvinceName=Arkansas/countryName=US
| Issuer: commonName=VeriSign Class 3 Secure Server CA - G3/organizationName=VeriSign,
Inc./countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2014-04-22 00:00:00
| Not valid after:  2017-06-19 23:59:59
| MD5:   87bb 6169 512f 0e5c 95bd a6f4 aa07 0ad5
|_SHA-1: 8d28 fc40 d476 d1b8 4613 c66e 6d4a 70e8 2218 3f96
```

Zenmap used to produce image

Load Balancer Detection

In order to determine if Dillards.com has a deployed load balancer two scans were used. The first tool used was ‘Load Balance Detector 0.2’, the second tool was ‘Halberd 0.2.3’. As the results indicate, a load balancer is deployed by Dillards.com.

Load Balancing Detector 0.2

Checking for DNS-Loadbalancing: NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: Ncat: Connection reset by peer.

FOUND

> HTTP/1.1 301 Moved Permanently

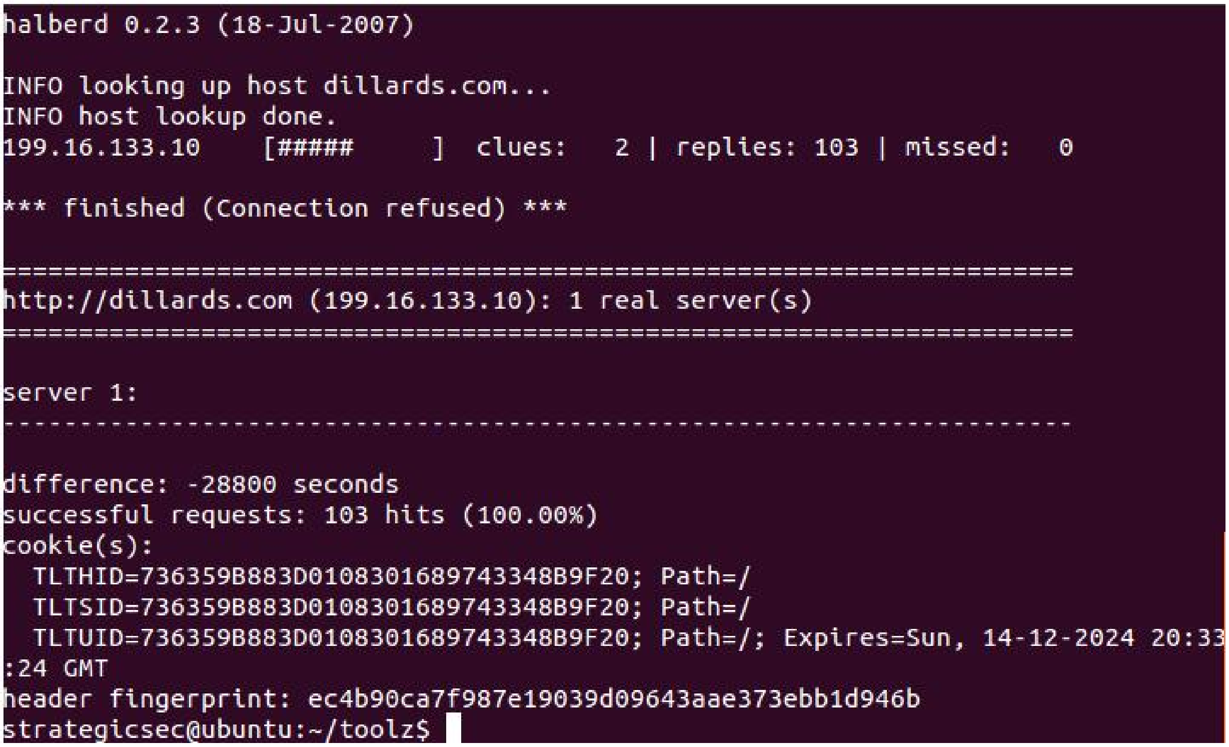
> Location: http://www.dillards.com/

> Connection: close

> Content-Type: text/html; charset=iso-8859-1

> dillards.com does Load-balancing. Found via Methods: HTTP[Diff]

Halberd 0.2.3



```
halberd 0.2.3 (18-Jul-2007)

INFO looking up host dillards.com...
INFO host lookup done.
199.16.133.10    [#####     ]  clues:   2 | replies: 103 | missed:   0

*** finished (Connection refused) ***

======================================================================
http://dillards.com (199.16.133.10): 1 real server(s)
======================================================================

server 1:
----------------------------------------------------------------------

difference: -28800 seconds
successful requests: 103 hits (100.00%)
cookie(s):
  TLTHID=736359B883D0108301689743348B9F20; Path=/
  TLTSID=736359B883D0108301689743348B9F20; Path=/
  TLTUID=736359B883D0108301689743348B9F20; Path=/; Expires=Sun, 14-12-2024 20:33
:24 GMT
header fingerprint: ec4b90ca7f987e19039d09643aae373ebb1d946b
strategicsec@ubuntu:~/toolz$
```

Email Address Discovery

Email Addresses Discovered

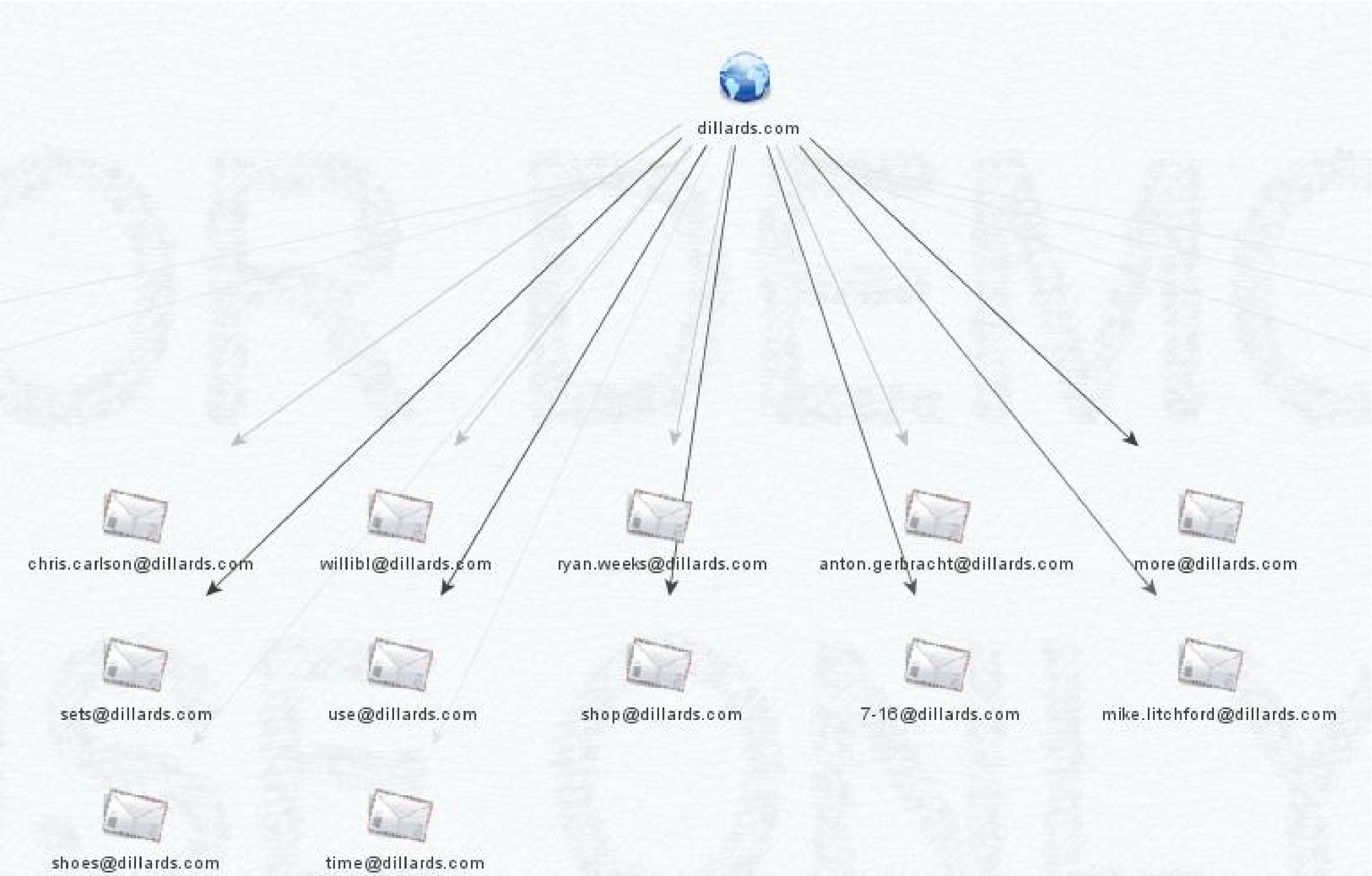
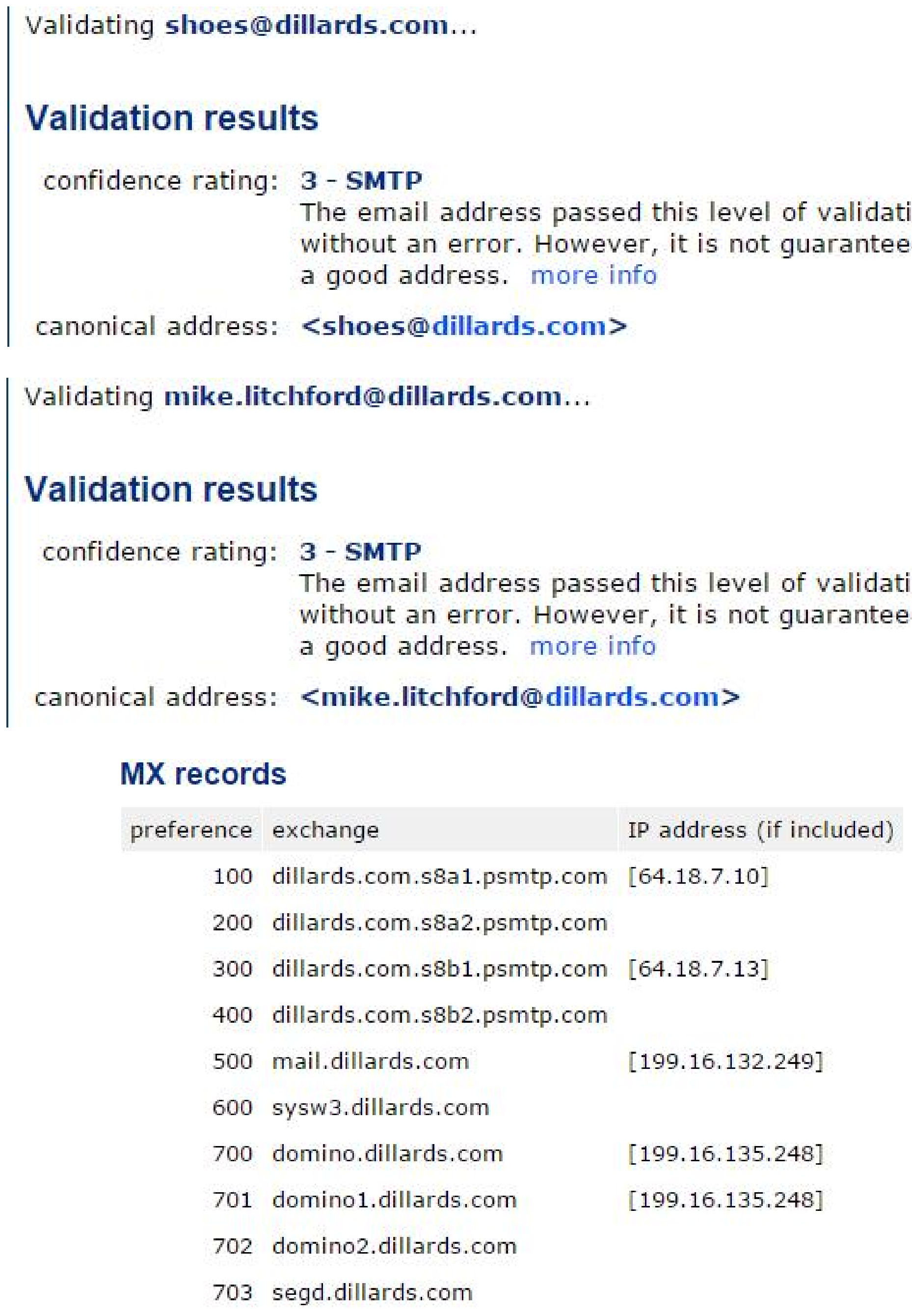


Image obtained using Maltego

Email Address Discovery

Active Email Discovery

Of the list of email addresses provided by Maltego a follow up was preformed to detect the active emails among those previously listed – two were confirmed active. The service used was Email Dossier hosted by Central Ops (centralops.com).



Validating **shoes@dillards.com**...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: **<shoes@dillards.com>**

Validating **mike.litchford@dillards.com**...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: **<mike.litchford@dillards.com>**

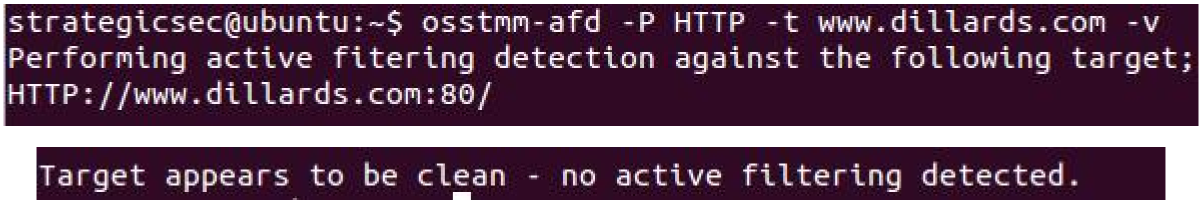
MX records

preference	exchange	IP address (if included)
100	dillards.com.s8a1.psmtp.com	[64.18.7.10]
200	dillards.com.s8a2.psmtp.com	
300	dillards.com.s8b1.psmtp.com	[64.18.7.13]
400	dillards.com.s8b2.psmtp.com	
500	mail.dillards.com	[199.16.132.249]
600	sysw3.dillards.com	
700	domino.dillards.com	[199.16.135.248]
701	domino1.dillards.com	[199.16.135.248]
702	domino2.dillards.com	
703	segd.dillards.com	

Intrusion Prevention Detection

IPS Detection

To find out if Dillards.com is running an IPS the open source script OSSTMM was used. The results show there is no IDS in place.

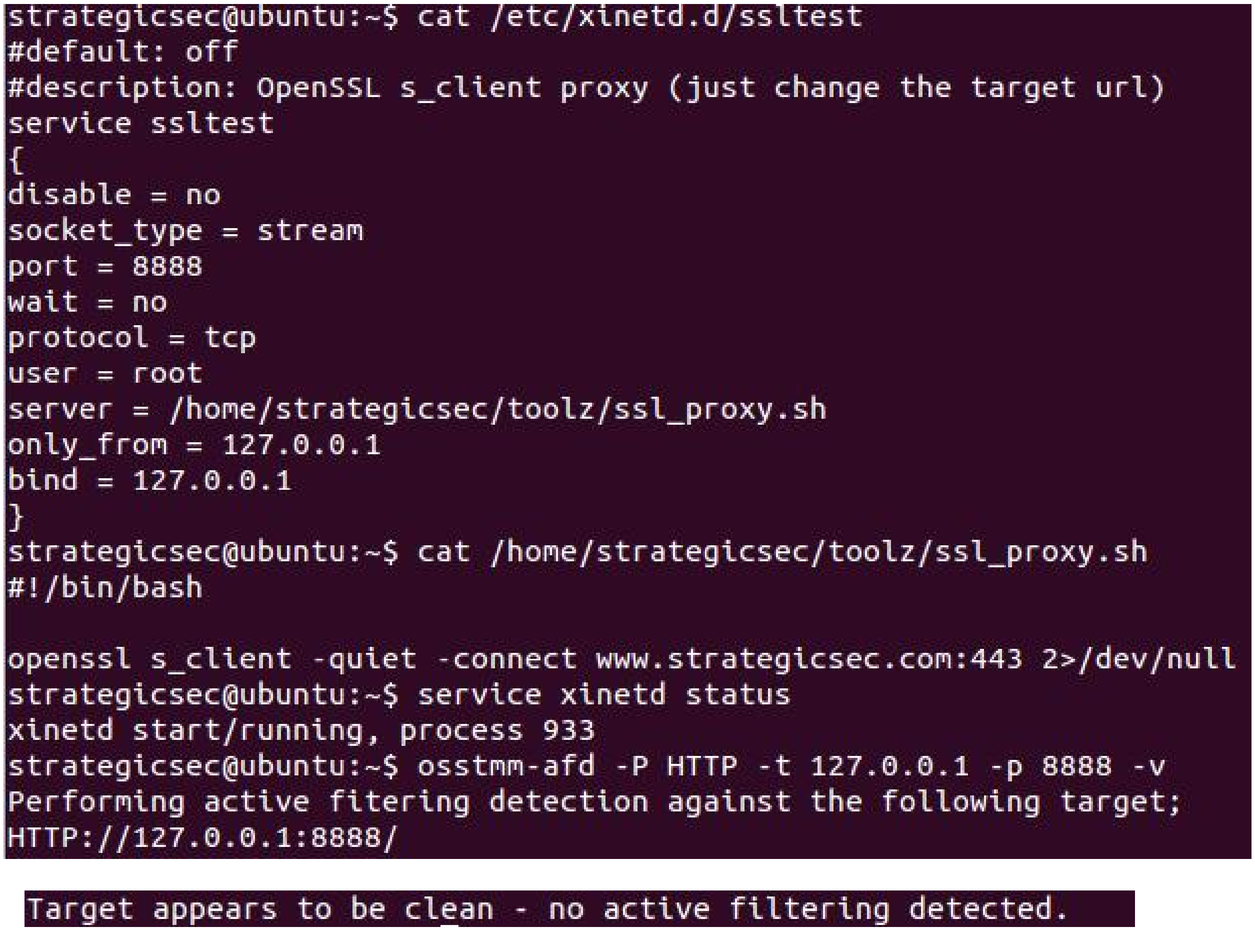


```
strategicsec@ubuntu:~$ osstmm-afd -P HTTP -t www.dillards.com -v
Performing active fitering detection against the following target;
HTTP://www.dillards.com:80/
```

```
Target appears to be clean - no active filtering detected.
```

Images taken of OSSTMM IPS detection script

No active filtering detected, a more advanced scan was preformed to confirm.

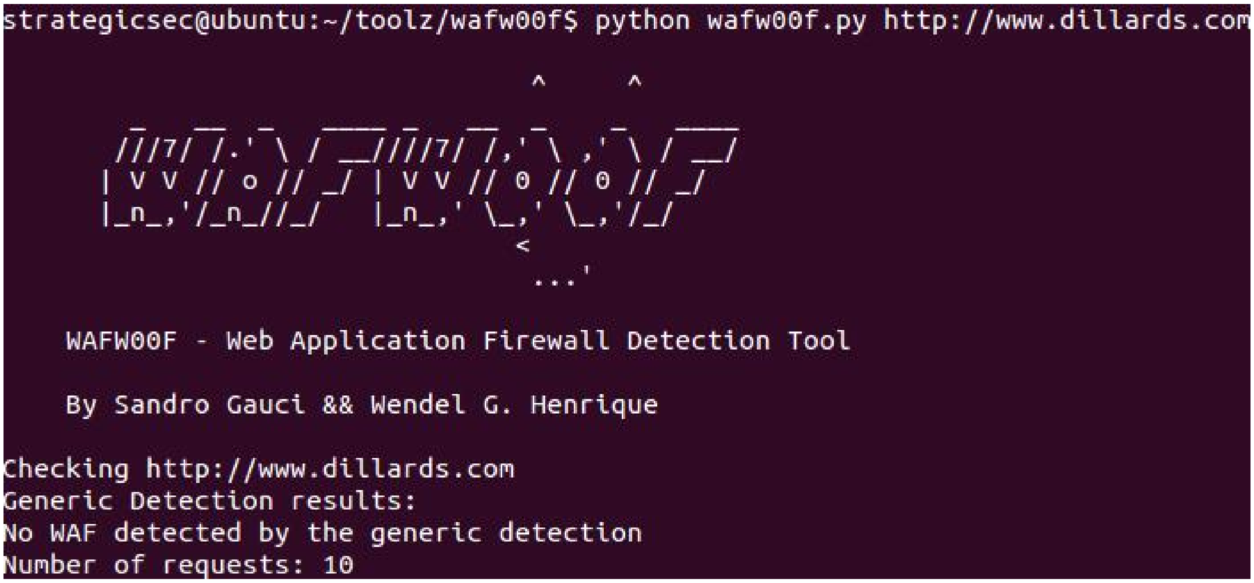


```
strategicsec@ubuntu:~$ cat /etc/xinetd.d/ssltest
#default: off
#description: OpenSSL s_client proxy (just change the target url)
service ssltest
{
disable = no
socket_type = stream
port = 8888
wait = no
protocol = tcp
user = root
server = /home/strategicsec/toolz/ssl_proxy.sh
only_from = 127.0.0.1
bind = 127.0.0.1
}
strategicsec@ubuntu:~$ cat /home/strategicsec/toolz/ssl_proxy.sh
#!/bin/bash

openssl s_client -quiet -connect www.strategicsec.com:443 2>/dev/null
strategicsec@ubuntu:~$ service xinetd status
xinetd start/running, process 933
strategicsec@ubuntu:~$ osstmm-afd -P HTTP -t 127.0.0.1 -p 8888 -v
Performing active fitering detection against the following target;
HTTP://127.0.0.1:8888/
```

```
Target appears to be clean - no active filtering detected.
```

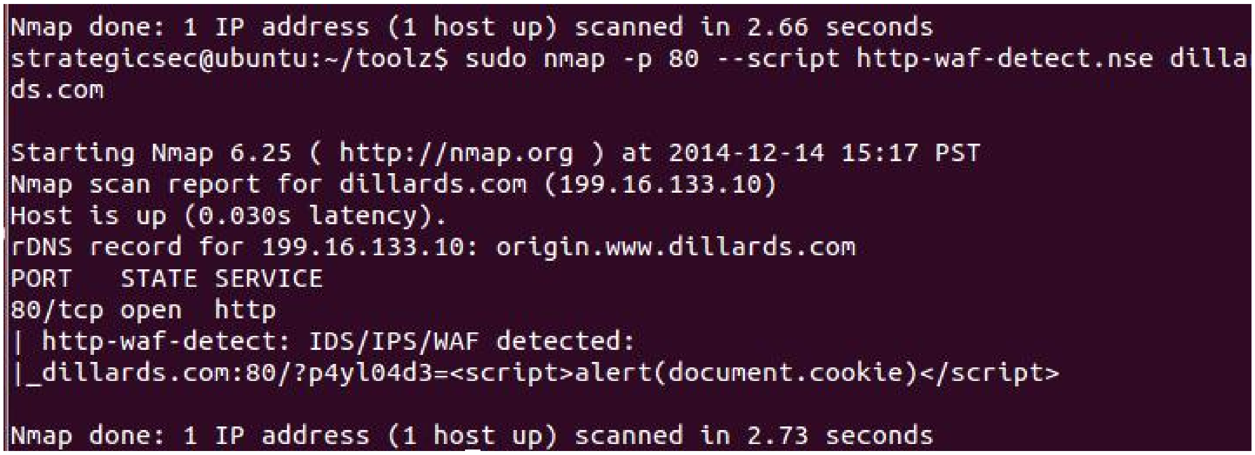
Images taken of OSSTMM IPS detection script

WAF Detection



```
strategicsec@ubuntu:~/toolz/wafw00f$ python wafw00f.py http://www.dillards.com

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://www.dillards.com
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 10
```

Image generated via WafWoof



```
Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
strategicsec@ubuntu:~/toolz$ sudo nmap -p 80 --script http-waf-detect.nse dilla
ds.com

Starting Nmap 6.25 ( http://nmap.org ) at 2014-12-14 15:17 PST
Nmap scan report for dillards.com (199.16.133.10)
Host is up (0.030s latency).
rDNS record for 199.16.133.10: origin.www.dillards.com
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_dillards.com:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 2.73 seconds
```

Image generated via Nmap