



# HUNTING ATTACKERS WITH NETWORK AUDIT TRAILS

John Pierce

[jpierce@lancope.com](mailto:jpierce@lancope.com)



# CREATING THE AUDIT TRAIL



# Network Auditing Basics

- Maximize Visibility
- Don't trust the host
- Store audit data in a central location
- Use a consistent format
- Use a consistent time stamp
- Be mindful of NAT and DHCP

## Improved Auditing

- Tie users to network data
- Store additional information like URLs, DNS, Application IDs
- Store complete connection records



# Creating the Trail

## Logging

- Provides user and application details
- Requires translation and aggregation
- Limited to configured hosts

## Packet Captures

- Provide complete network record and unencrypted content
- Large storage requirement limits visibility or retention length
- Difficult to search

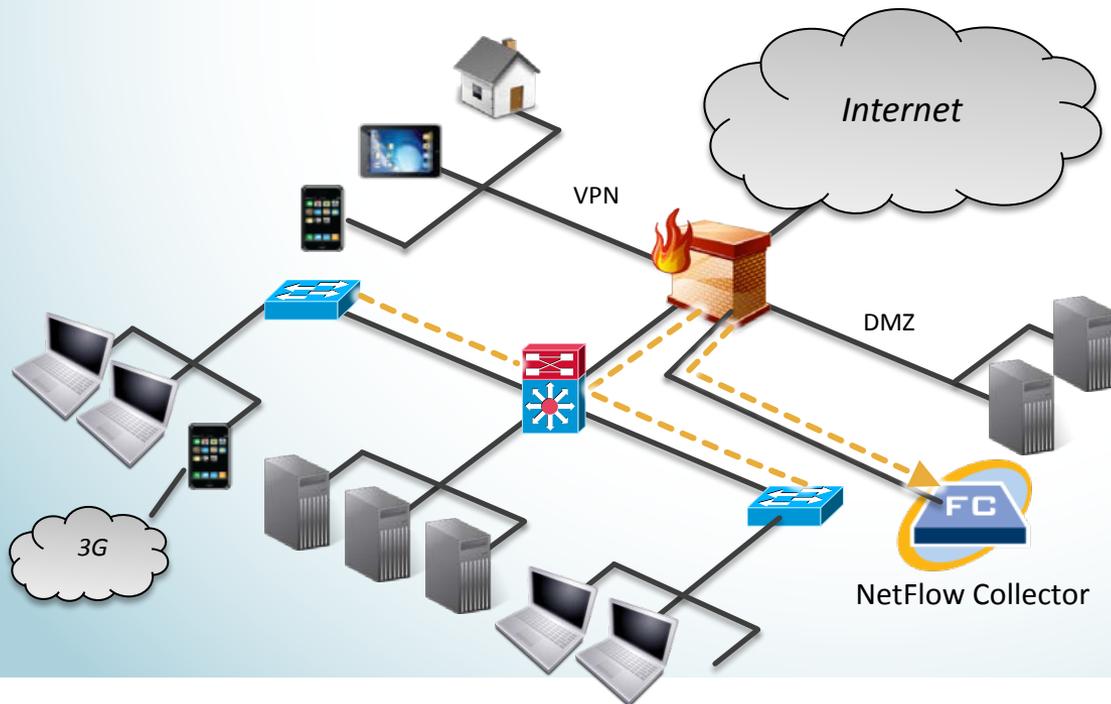


# NETFLOW



# Netflow Basics

- Does not require host level configuration
- Devices with one or more Flow producing interfaces are “Exporters”
- Exporters cache and forward records to “Collectors”
- Common Exporters include firewalls, switches, and routers



## NetFlow Packets

src and dst ip
src and dst port
start time
end time
mac address
byte count
- more -



# Transactional Audits of ALL activities

Item	Day	Date	Time	Number Called	Call To	Min	Rate Code	Rate Pd	Feature	Airtime Charge	LD/Add'l Charge	Total Charge
1	WED	02/17/2010	9:09AM	770-364	INCOMING CL	2	7ESM	DT	M2MC	0.00	0.00	0.00
2	WED	02/17/2010	1:48PM	678-777	INCOMING CL	5	7ESM	DT	M2MC	0.00	0.00	0.00
3	THU	02/18/2010	11:01AM	213-447	LOSANGELE CA	1	7ESM	DT	M2MC	0.00	0.00	0.00
4	THU	02/18/2010	3:46PM	404-519	ATLANTA GA	5	7ESM	DT	M2MC	0.00	0.00	0.00
5	THU	02/18/2010	5:30PM	678-777								
6	THU	02/18/2010	6:30PM	678-777								

• Much like a phone bill

Flow Table - 880 records

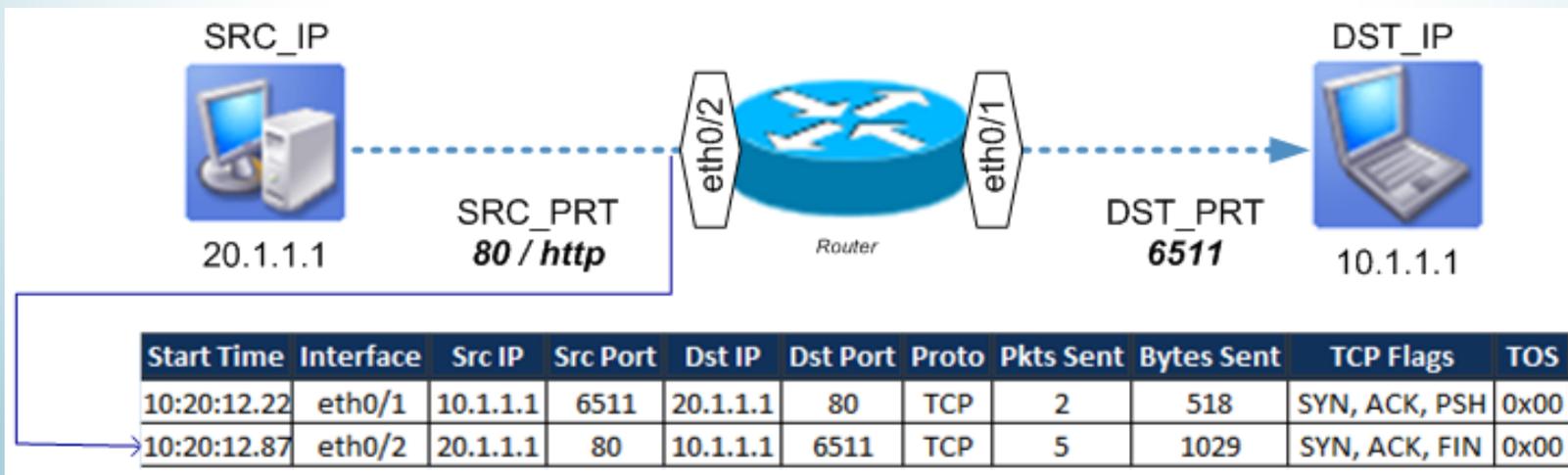
Start Active Time	Client Host	Client Zone	Server Host	Server Zone	Service Summary
Apr 12, 2010 8:41:56 AM (6 hours 32 minutes 10s ago)	10.201.3.96	Sales and Marketing	72.21.202.71	United States	http (80/tcp)
Apr 12, 2010 8:43:14 AM (6 hours 30 minutes 52s ago)	10.201.3.96	Sales and Marketing	216.165.129.141	United States	http (80/tcp)
Apr 12, 2010 8:45:51 AM (6 hours 28 minutes 15s ago)	10.201.3.96	Sales and Marketing	68.142.118.82	LimeLight Networks	http (80/tcp)
Apr 12, 2010 8:43:34 AM (6 hours 30 minutes 32s ago)	10.201.3.96	Sales and Marketing	72.21.202.96	United States	http (80/tcp)
Apr 12, 2010 6:52:48 AM (8 hours 21 minutes 18s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)
Apr 12, 2010 7:22:53 AM (7 hours 51 minutes 13s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)
Apr 12, 2010 12:13:13 PM (3 hours 53s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)
Apr 12, 2010 9:02:34 AM (6 hours 11 minutes 32s ago)	10.201.3.96	Sales and Marketing	72.233.96.254	United States	http (80/tcp)
Apr 12, 2010 8:43:36 AM (6 hours 30 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.167.164.64	United States	http (80/tcp)
Apr 12, 2010 8:57:33 AM (6 hours 16 minutes 33s ago)	10.201.3.96	Sales and Marketing	72.21.202.165	United States	http (80/tcp)
Apr 12, 2010 10:16:50 AM (4 hours 57 minutes 16s ago)	10.201.3.96	Sales and Marketing	10.201.0.15	Sales and Marketing	ldap (389/tcp)
Apr 12, 2010 8:43:35 AM (6 hours 30 minutes 31s ago)	10.201.3.96	Sales and Marketing	63.245.217.21	United States	http (80/tcp)
Apr 12, 2010 2:59:36 PM (14 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http (80/tcp)
Apr 12, 2010 8:43:09 AM (6 hours 30 minutes 57s ago)	10.201.3.96	Sales and Marketing	63.245.209.115	United States	https (443/tcp)



# Logging Standards

- NetFlow v9 (RFC-3950)
- IPFIX (RFC-5101)
- Rebranded NetFlow
  - Jflow – Juniper
  - Cflowd – Juniper/Alcatel-Lucent
  - NetStream – 3Com/Huawei
  - Rflow – Ericsson
  - AppFlow - Citrix

## Basic/Common Fields



# Extensible Data Fields



**Data sources can provide additional log information**

## **Examples of Extensible Fields**

- Network Based Application Recognition
- Performance Metrics (SRT/RRT, Collisions)
- HTTP Headers
- NAT Data
- Security Action (Permit/Deny)
- TTL
- DSCP
- Payload

# Stitching & De-duplication



- 1 Connection
- 3 Exporters
- 6 Interfaces
- 12 Flow entries

Each exporter interface provides a unique view of the connection

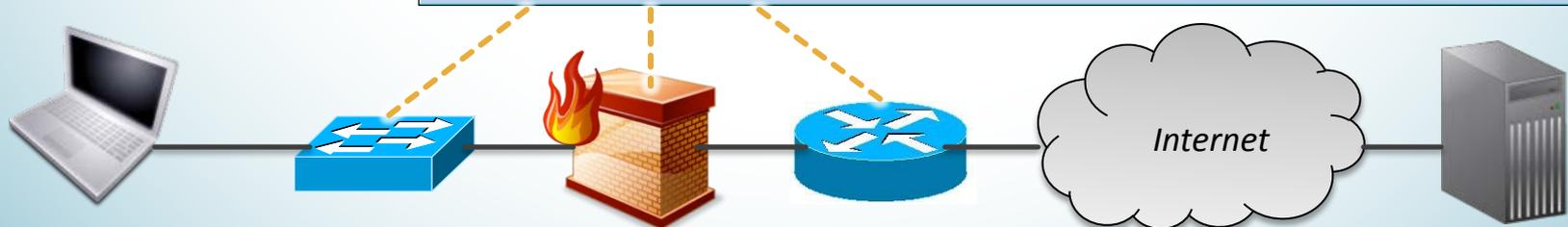
Quick View for Flow

Client Exporters IP (IF)

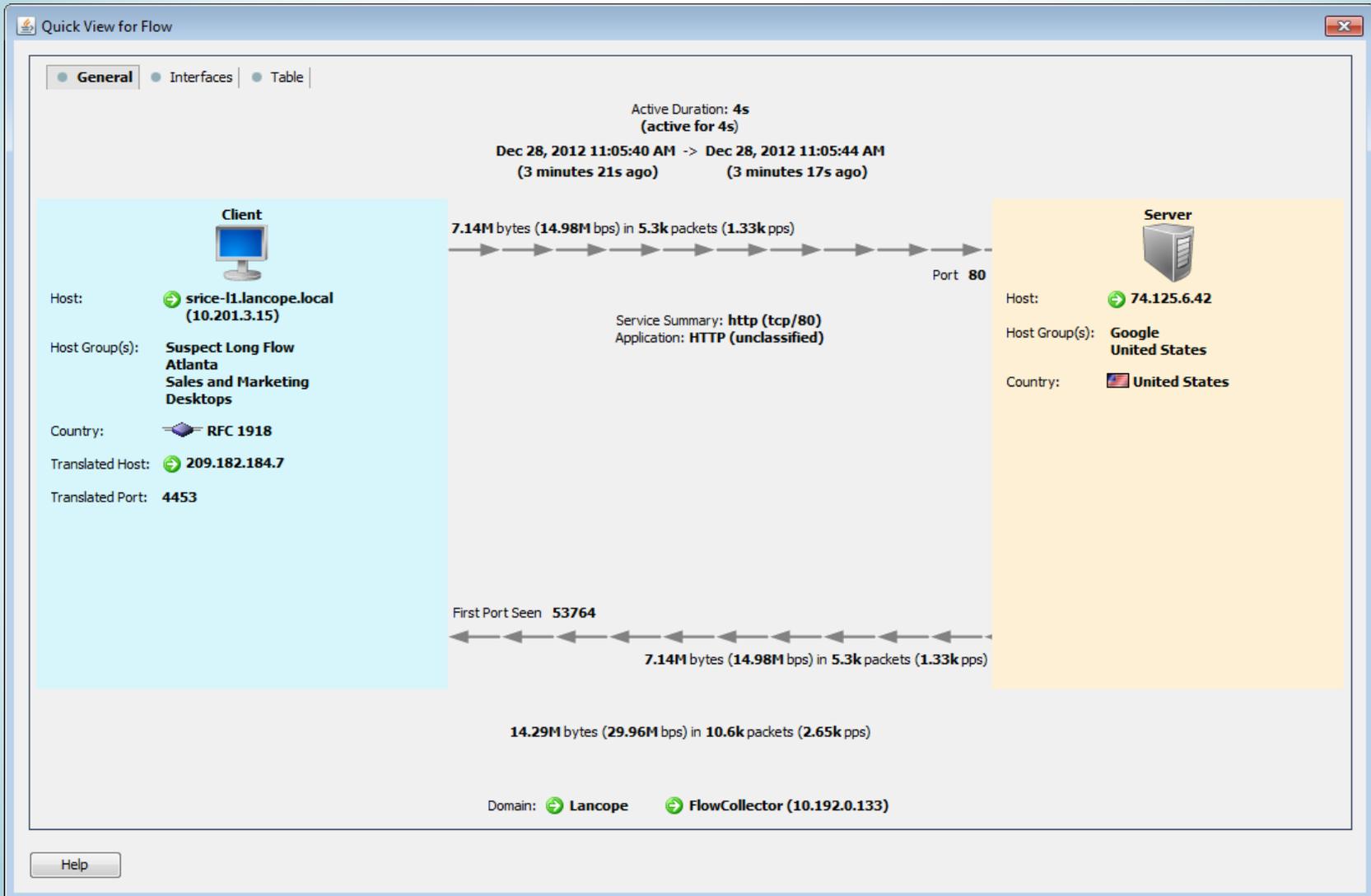
Server Exporters IP (IF)

Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Outbound		best_effort	
10.240.200.2	Exporter	ifIndex-2	Inbound			
10.240.200.1	Cisco ASA	Wan	Outbound			Permitted
10.240.200.1	Cisco ASA	Lan	Inbound			Permitted
lchggw01.lancc (10.201.0.1)	Exporter	Vlan1	Inbound		best_effort	
lchggw01.lancc (10.201.0.1)	Exporter	Vlan240	Outbound			

Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Inbound		best_effort	
10.240.200.2	Exporter	ifIndex-2	Outbound			
10.240.200.1	Cisco ASA	Wan	Inbound			Permitted
10.240.200.1	Cisco ASA	Lan	Outbound			Permitted
lchggw01.lancc (10.201.0.1)	Exporter	Vlan1	Outbound			
lchggw01.lancc (10.201.0.1)	Exporter	Vlan240	Inbound		best_effort	



# Stitching & De-duplication





# NETFLOW TOOLS



# SiLK

- Download at <http://tools.netsa.cert.org>
- Stores and processes flow
- Project Managed by Carnegie Mellon CERT

Query Builder (demo-0f0z.isilk)

Basic Query Options | More Filter Options

Data files to search  
Data Pool (class/type) Incoming  
Sensors All Sensors Choose...

Time Range to Query  
Current Hour  
Apr Apr

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Start hour (GMT): 20 End hour (GMT): 20  
Selected 1 hour

IP Addresses and Ports  
 Filter based on source and destination

Source  
IP x.x.x.x  
IP Set (Choose a set)  
Port 0-65535

Destination  
IP x.x.x.x  
IP Set (Choose a set)  
Port 0-65535

```
rxfilter --type=in,web --start-date=2013/04/22:20 --proto=0-255 --pass=#output
```

Name Untitled Query Add to demo-0f0z.isilk  Return records that FAIL filter

Validate Options Save As Plugin... Close Run Remote Query

isilk 0.1.0 - wbha.isilk - ajk@172.16.230.2:/output/kompaneawbha.isilk

File Edit Tools Graph View Help

Query Info Files rxfilter rxfset rxfung rxfcount Quick-Graph shell

wbha.isilk

- Untitled Query
- Untitled rxfung result
- Graph - Bytes
- Graph - Packets
- Untitled rxfcount time-series
- Count Graph

Count Graph  
(No command line)  
Local file: C:\Documents and Settings\Administrator\My Documents\isilk\wbha.isilk\Count\_Graph-197.png.asc

15 19:20 2004/12/15 20:35 2004/12/15 21:50 2004/12/15 23:05 2004/12/15

213 records - C:\Documents and Settings\Administrator\My Documents\isilk\wbha.isilk\Untitled\_rxfcount\_time-series-5c9u.asc

# PySiLK



```
# Import the global variables needed for processing the record
global smtpports, counts

# Pull data from the record
sip = rec.sip
bytes = rec.bytes

# Get a reference to the current data on the IP address in question
data = counts.setdefault(sip, [0, 0])

# Update the total byte count for the IP address
data[0] += bytes

# Is the flow mail related? If so add the byte count to the mail bytes
if (rec.protocol == 6 and rec.sport in smtpports and
    rec.packets > 3 and rec.bytes > 120):
    data[1] += bytes
    return True

# If not mail related, fail the record
return False
```



# Commercial Solutions

- Arbor PeakFlow
- IBM Qradar
- Invea-Tech FlowMon
- Lancope StealthWatch
- ManageEngine
- McAfee NTBA
- Plixer Scrutinizer
- ProQSys FlowTraQ
- Riverbed Cascade (formerly Mazu)

\* For comparison see Gartner Network Behavior Analysis Market December 2012 (G00245584)



# NETWORK AUDIT LOG DETECTION



# Signature Matching

- IP Blacklists / IP Reputation
- Match Indicators Of Compromise for stored values
- Policy Enforcement
- Measure Compliance

# What can you detect with the audit log?



## Reveal BotNet Hosts

	Policy	Start Active Time	Source	Source Host Groups	Target	Target Country	Target Host Groups	Details
	Inside Hosts	Feb 11, 2013 2:40:00 PM (1 hour 53 minutes 27s ago)	209.182.184.8	Atlanta	ns1.dns-domainserve (82.208.40.4)	Czech Republic	Czech Republic, Zeus	Successful communication was detected between this inside host and C&C server using port 80 and the TCP protocol, and <a href="http://host1.fileserv.uni.me/css...">http://host1.fileserv.uni.me/css...</a>

↑  
Layer 3

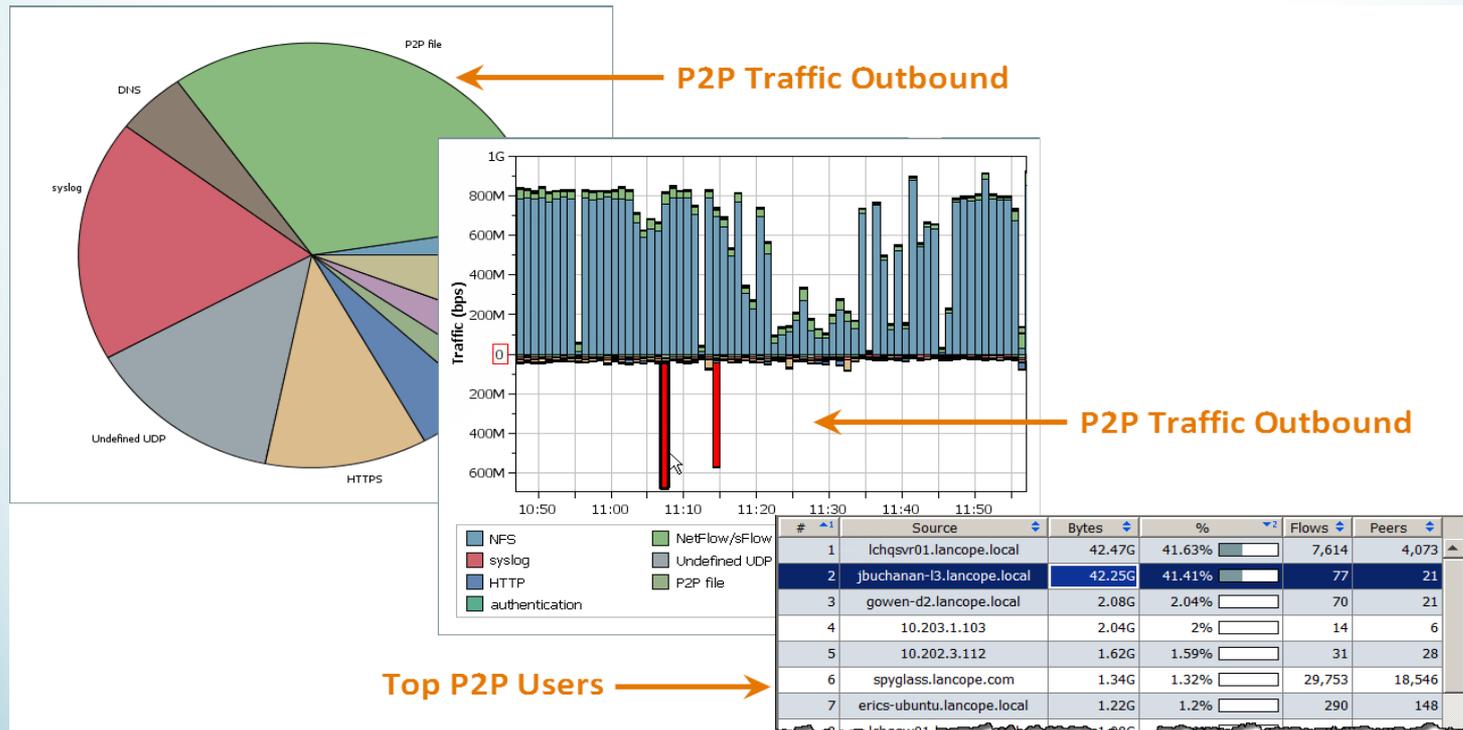
↑  
Layer 4  
and URL



# What can you detect with the audit log?

## Unsanctioned Device and Application Detection

- ▶ Identify the use of unsanctioned applications
- ▶ Detect rogue servers and other rogue devices





# Firewall Policy Monitoring And Enforcement

- ▶ Audit Firewall rules
- ▶ Immediately detect misconfigurations
- ▶ Enforce policy between hosts on the same segment

**Quick View for Flow**

Active Duration: 2 minutes 2s (active for 2 minutes 2s)  
2011/5/4 08:35:08 -> 2011/5/4 08:37:10  
(5 minutes 59s ago) (3 minutes 57s ago)

**Client**  
Host: 10.10.10.10,65  
Host Group(s): Networks  
Country: United States

2.19k bytes (147.15 bps) in 18 pac  
Port: 53

Service Summary: dnstcp (tcp/53)  
Application: SSH  
1 TCP Connection

First Port Seen: 11669

75.74 bps in 15 packets (0.98 pps)

**Server**  
Host: 10.10.10.10,40  
Host Group(s): Taiwan Suspicious Internet Hosts  
Country: Taiwan  
SRT Average: 12 ms  
Payload: SSH-1.99-OpenSSH\_4.5p1 Fre

Host Locking Configuration for Domain "NinjaNet"

ID	Rule Name	Client Host Group	Server Host Group	Allow/Disallow	Exceptions
5	Restrict Administrative Access	Internal Network	PCI Zone	Disallow All	Services: https, sftp, ssh

Buttons: Add, Remove, Duplicate, Edit, Reverse, Import, Export, Help, Apply, Close, OK



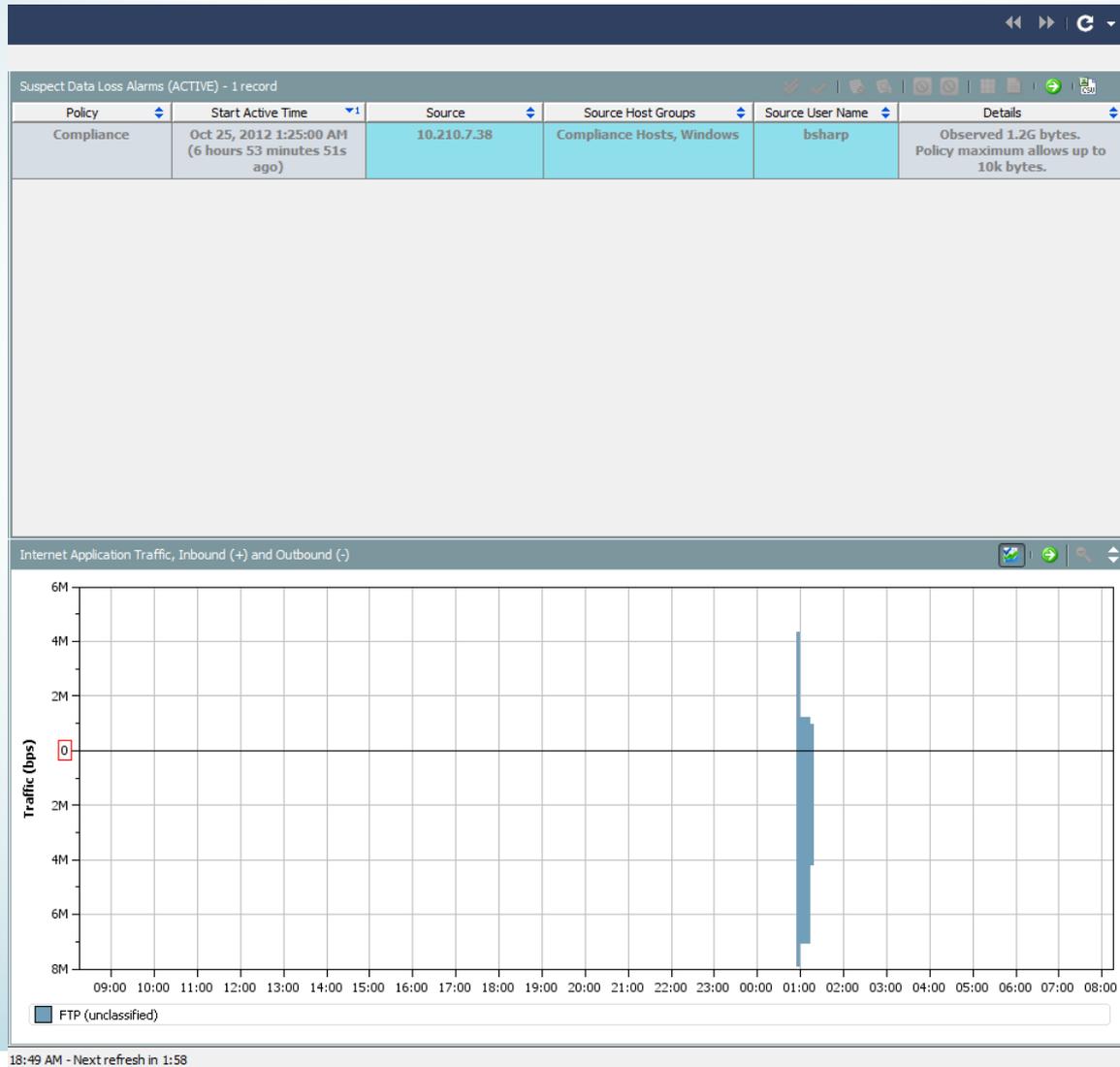
# Intelligent Analysis

- Data Exfiltration/Collection
- Internal Pivot
- Worm Propagation
- Covert Channels
- Abnormal Behavior

# What Can Intelligent NetFlow Analysis Do?



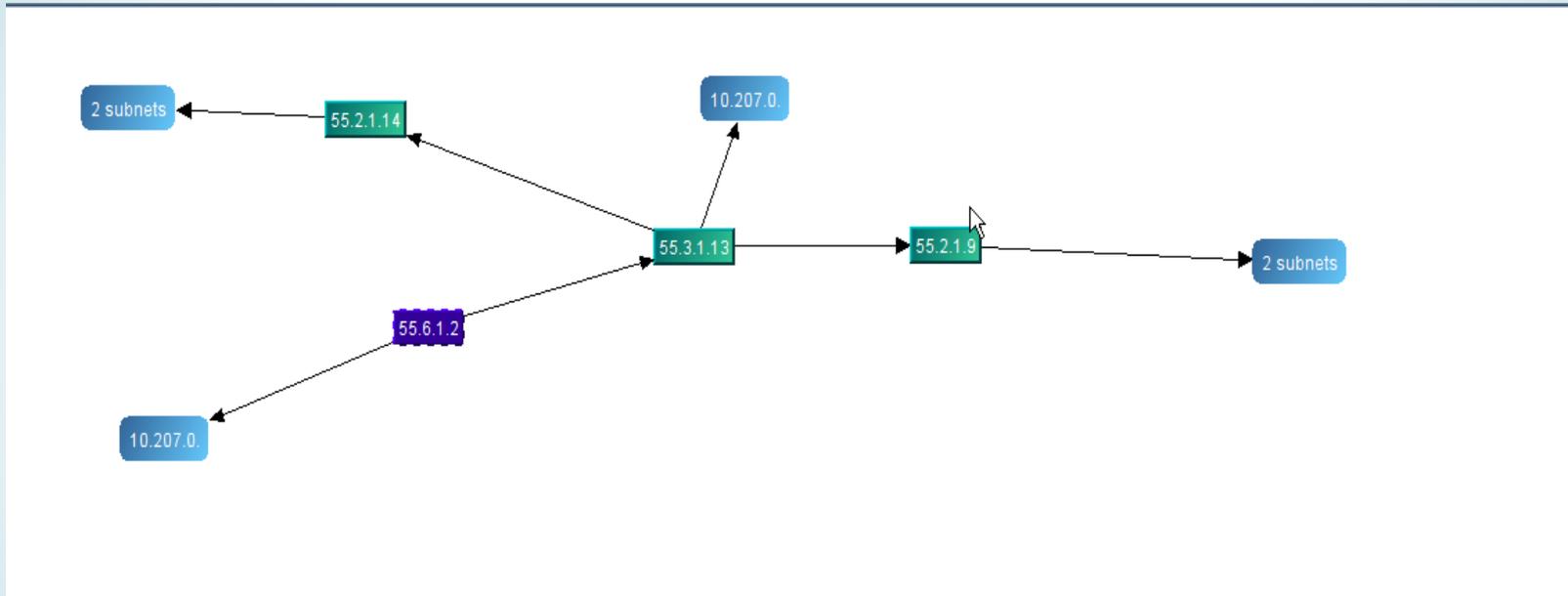
## Loss of Protected Data



# What Can Intelligent NetFlow Analysis Do?



## Track Malware Propagation



Details - 2 records

Earliest Time	Port	Protocol	Next Hop	Total Hosts Subnet	Propagated Hosts Subnet
05/22/08 01:15:59	445	tcp	55.3.1.13	3	17
05/22/08 01:16:09	445	tcp	Subnet 10.207.0.	1	

# What Can Intelligent NetFlow Analysis Do?



## Reveal Recon

<span>Internal Spreading Malware</span> <span>Bot Detection</span> <span>Suspect Data Loss</span> <span>Policy Violation</span> <span>Reconnaissance Detection</span> <span>DDoS Detection</span> <span>Alarms</span>				
Concern Index - 16 records summarized into 16 records				
Host Groups	Host	CI	CI%	Alerts
Atlanta	spyglass.lancope.com (209.182.184.2)	3,520,636	1,174%	Excess_Clients, Port_Scan
Atlanta	209.182.184.1	26,888,520	269%	Rejects, UDP_Scan
Sales and Marketing, Atlanta, Users, Windows	jbuchanan-d2.lancope.local (10.201.3.24)	15,995,525	160%	TCP_Scan
New York, Windows	10.90.10.254	9,132,249	91%	TCP_Scan
New York, Windows	10.30.10.254	8,312,191	83%	TCP_Scan
New York, Windows	10.40.10.254	8,329,626	83%	TCP_Scan
New York, Windows	10.80.10.254	8,344,656	83%	TCP_Scan
New York, Windows	10.70.10.254	8,182,332	82%	TCP_Scan
New York, Windows	10.50.10.254	8,074,116	81%	TCP_Scan
New York, Windows	10.100.10.254	8,020,008	80%	TCP_Scan
New York, Windows	10.20.10.254	7,686,342	77%	TCP_Scan
New York	10.110.10.254	7,608,186	76%	TCP_Scan
New York, Windows	10.60.10.254	7,202,376	72%	TCP_Scan
Atlanta	209.182.176.42	2,144,863	67%	Rejects
SG Private	lcsgrw01.lancope.local (10.192.0.1)	5,972,924	60%	Ping, Ping_Oversized_Packet, Ping_Scan, Rejects
Sales and Marketing, Atlanta, Users, Windows	10.201.3.83	5,903,806	59%	Ping_Oversized_Packet, TCP_Scan



# **FORENSIC INVESTIGATIONS USING THE NETWORK AUDIT TRAIL**



# The Five W's

- Who did this?
- What did they do?
- When did it happen?
- Where did they go inside my network?
- Why are they inside?



# Who

- External IP/DNS (C&C server, Watering Hole)
- Internal IP (DMCA notice, Bot notification)

## Look for:

- Assets touching that address
- Activity on those Assets post contact
- Services used in the contact / post contact
- Geo location on the external addresses



# What

- Self replicating Malware
- Data Exfiltration
- Suspect covert channel

Look for:

- Analyze service usage across the network
- Look for strange Bytes per Connection (too large, small, or regular as appropriate)
- Look for reverse tunnels
- Look for very long connections



# When

- Analysis should cover everything from the recon phase to today
- If intrusion/infection detected, all actions of that machine should be analyzed from initial intrusion to verified clean state

Look for:

- Even after you think you have removed the intruder's presence, continue to look for IOC.



# Where

- As you uncover new information (IP addresses, countries of origin, exploited services) – search your whole data set for the new IOC
- Analyze all relationships between infected/compromised host and your other assets

Look for:

- Be mindful- the intrusion you have observed may not be the first.



# Why

- Are they after your resources or your data?
- If information was publicly disclosed, where does that info exist in your network? Also, who had access and may have stored local copies?

Look for:

- How data could have left your network
- What other resources/data may have been attractive to the attacker



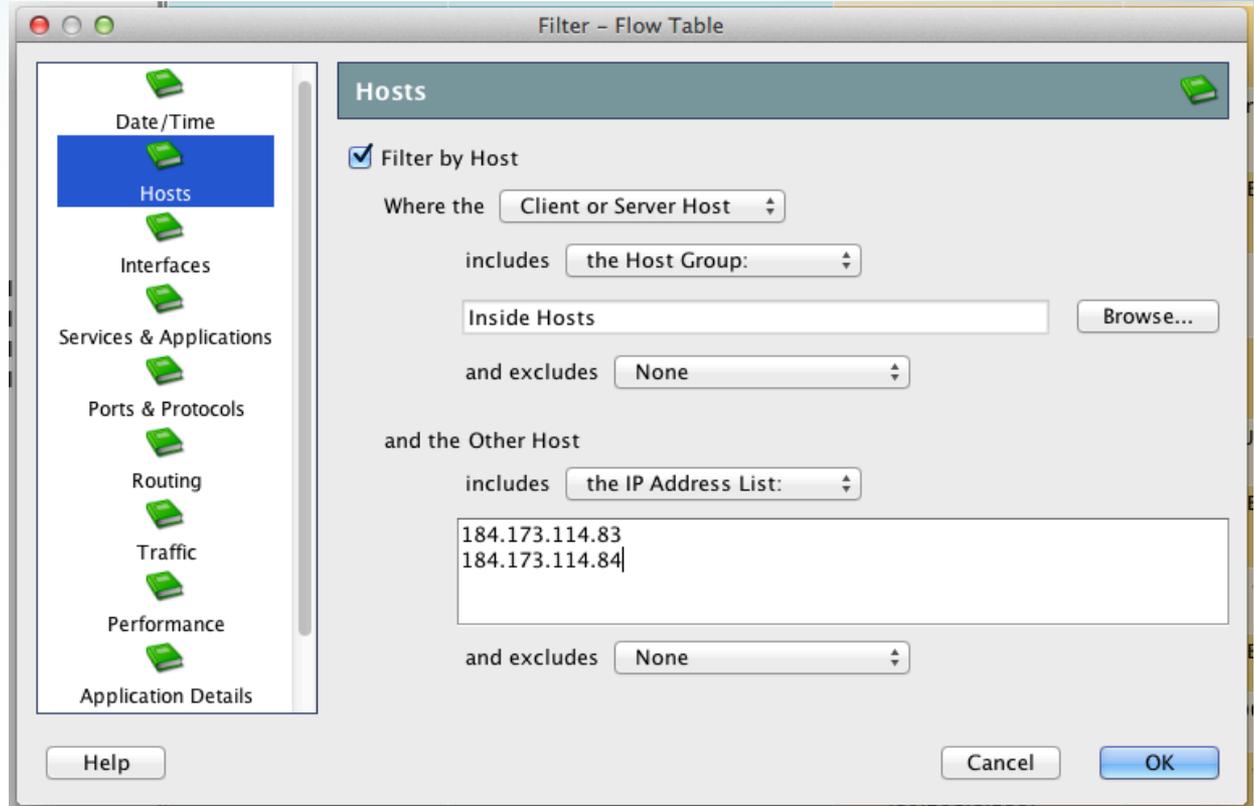
# PUTTING IT TOGETHER

# Following IOC



Waterhole campaign targeting your industry has been publicly disclosed.

A quick search of your network audit trail reveals an internal host that accessed the disclosed site.



Filter Domain : Default Domain Time : Last 1 day  
Client or Server Host Group : Inside Hosts  
Client or Server Hosts : 2 Hosts

Table Short List

Flow Table - 1 record

Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application	Service Summary	Total Tr...	Total Bytes	Tc
10.15.165	Catch All	184.173.114.84-static.revers (184.173.114.84)	United States	1s	HTTP (unclassified)	http (80/tcp)	9.55k	1.17k	Tc

# Following IOC



## Check host details around that time

Filter Domain : Default Domain Time : Last 4 hours  
Client or Server Host : 10.201.15.165

Table Short List

Flow Table - 78 records

Client Host	Server Host	Server Host Groups	Duration	Application	Service Summary	Total Tr...	Total Bytes	Total Packets	Start Active Time	Client Bytes	Client Ratio (%)	Server Bytes
10.15.165	(209.20.87.227)	United States	4 minutes 15s	HTTP (unclassified)	http (80/tcp)	603	18.8k	35	May 14, 2013 8:34:37 AM (1 hour 1 minute 51s ago)	1.11k	5.89%	17
10.15.165	fs16.trilulilu.ro (89.33.207.35)	Romania	9 minutes 26s	HTTP (unclassified)	http (80/tcp)	67	4.66k	15	May 14, 2013 8:35:11 AM (1 hour 1 minute 17s ago)	638	13.36%	4
10.15.165	www.trilulilu.ro (89.33.207.37)	Romania	< 1s	HTTP (unclassified)	http (80/tcp)	34.38k	4.2k	12	May 14, 2013 8:35:21 AM (1 hour 1 minute 7s ago)	584	13.59%	3
10.15.165	li69-45.members.linode.com (74.207.227.45)	United States	4 minutes 37s	Undefined TCP	Undefined TCP (11942/tcp)	218.69k	7.22M	7,848	May 14, 2013 8:36:39 AM (59 minutes 49s ago)	132.2k	1.79%	7
10.15.165	li69-45.members.linode.com (74.207.227.45)	United States	16 minutes 36s	SSH/SCP (unclassified)	ssh (22/tcp)	13.81k	1.64M	2,906	May 14, 2013 8:39:20 AM (57 minutes 8s ago)	1.54M	93.85%	103
10.15.165	yn-in-f113.1e100.net (74.125.139.113)	United States	< 1s	HTTP (unclassified)	http (80/tcp)	10.84k	1.32k	11	May 14, 2013 8:41:34 AM (54 minutes 54s ago)	501	36.97%	6
10.15.165	yn-in-f99.1e100.net (74.125.139.99)	United States	2 minutes 27s	HTTP (unclassified)	http (80/tcp)	465	8.35k	31	May 14, 2013 8:41:36 AM (54 minutes 52s ago)	1.43k	17.15%	6
10.15.165	yn-in-f103.1e100.net (74.125.139.103)	United States	9 minutes 58s	HTTP (unclassified)	http (80/tcp)	468	34.21k	80	May 14, 2013 8:42:50 AM (53 minutes 38s ago)	3.33k	9.73%	30
10.15.165	yn-in-f105.1e100.net (74.125.139.105)	United States	5 minutes 48s	HTTP (unclassified)	http (80/tcp)	1.35k	57.51k	102	May 14, 2013 8:43:07 AM (53 minutes 21s ago)	3.53k	6.14%	53
10.15.165	yn-in-f147.1e100.net (74.125.139.147)	United States	< 1s	HTTP (unclassified)	http (80/tcp)	11.26k	1.38k	11	May 14, 2013 8:43:13 AM (53 minutes 15s ago)	618	43.89%	6
10.15.165	63.241.153.51	United States	< 1s	HTTP (unclassified)	http (80/tcp)	59.63k	7.28k	17	May 14, 2013 8:43:15 AM (53 minutes 13s ago)	664	8.91%	6
10.15.165	a184-26-136-104.deploy.akamaitechnologies.com (184.26.136.104)	United States	9 minutes 27s	HTTP (unclassified)	http (80/tcp)	682	47.21k	85	May 14, 2013 8:43:27 AM (53 minutes 1s ago)	2.44k	5.17%	4

## Suspicious HTTP connections right after contact- good candidate for a drive-by download

(209.20.87.227)	United States	4 minutes 15s	HTTP (unclassified)	http (80/tcp)	603	18.8k	35	May 14, 2013 8:34:37 AM (1 hour 1 minute 51s ago)
fs16.trilulilu.ro (89.33.207.35)	Romania	9 minutes 26s	HTTP (unclassified)	http (80/tcp)	67	4.66k	15	May 14, 2013 8:35:11 AM (1 hour 1 minute 17s ago)
www.trilulilu.ro (89.33.207.37)	Romania	< 1s	HTTP (unclassified)	http (80/tcp)	34.38k	4.2k	12	May 14, 2013 8:35:21 AM (1 hour 1 minute 7s ago)

## Suspicious download followed by a reverse SSH shell. Most SSH bytes sent by "client"

li69-45.members.linode.com (74.207.227.45)	United States	4 minutes 37s	Undefined TCP	Undefined TCP (11942/tcp)	218.69k	7.22M	7,848	May 14, 2013 8:36:39 AM (59 minutes 49s ago)	132.2k	1.79%
li69-45.members.linode.com (74.207.227.45)	United States	16 minutes 36s	SSH/SCP (unclassified)	ssh (22/tcp)	13.81k	1.64M	2,906	May 14, 2013 8:39:20 AM (57 minutes 8s ago)	1.54M	93.85%

# Following IOC



Attacker reconns your network. Investigate any hosts contacted by the compromised host. Additionally- look for any other hosts scanning for 445 and 135.

Filter Domain : Default Domain Time : Last  
Client or Server Host : 10.201.15.165

Table Short List

Flow Table - 78 records

Client Host	Server Host	Duration	Application	Service Summary	Total Tr...	Total Bytes	Total Packets	Start Active Time
10.201.15.165	10.201.15.31	< 1s	SMB (unclassified)	smb (445/tcp)	368	46	1	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.30	< 1s	SMB (unclassified)	smb (445/tcp)	368	46	1	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.68	< 1s	SMB (unclassified)	smb (445/tcp)	368	46	1	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.82	< 1s	SMB (unclassified)	smb (445/tcp)	368	46	1	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.86	< 1s	SMB (unclassified)	smb (445/tcp)	368	46	1	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.32	< 1s	SMB (unclassified)	smb (445/tcp)	736	92	2	May 14, 2013 8:54:07 AM (42 minutes 21s ago)
10.201.15.165	10.201.15.82	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.87	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.86	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.30	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.68	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.32	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)
10.201.15.165	10.201.15.31	< 1s	MS-RPC (unclassified)	ms-rpc (135/tcp)	368	46	1	May 14, 2013 8:55:29 AM (40 minutes 59s ago)

## Following IOC



Since we have uncovered a new IOC (IP address controlling the reverse SSH shell), we should check to see if that host has touched the network anywhere else.

Filter Domain : Default Domain Time : Last 2 days  
Client or Server Host Group : Inside Hosts  
Client or Server Host : li69-45.members.linode.com (74.207.227.45)

Table Short List

Flow Table - 10 records

Client Host	Server Host	Duration	Application	Service Summary	Total Bytes	Start Active Time	Client Bytes	Client Ratio (%)
10.1.15.159	li69-45.members.linode.com (74.207.227.45)	1 minute 36s	SSH/SCP (unclassified)	ssh (22/tcp)	219.72M	May 14, 2013 7:45:40 AM (1 day 1 hour 45 minutes ago)	215.23M	97.96%
10.1.15.159	li69-45.members.linode.com (74.207.227.45)	20s	SSH/SCP (unclassified)	ssh (22/tcp)	18.5M	May 14, 2013 7:35:16 AM (1 day 1 hour 55 minutes ago)	18.1M	97.84%
10.1.15.159	li69-45.members.linode.com (74.207.227.45)	2 minutes 38s	SSH/SCP (unclassified)	ssh (22/tcp)	135.84k	May 14, 2013 7:23:10 AM (1 day 2 hours 7 minutes ago)	110.47k	81.32%

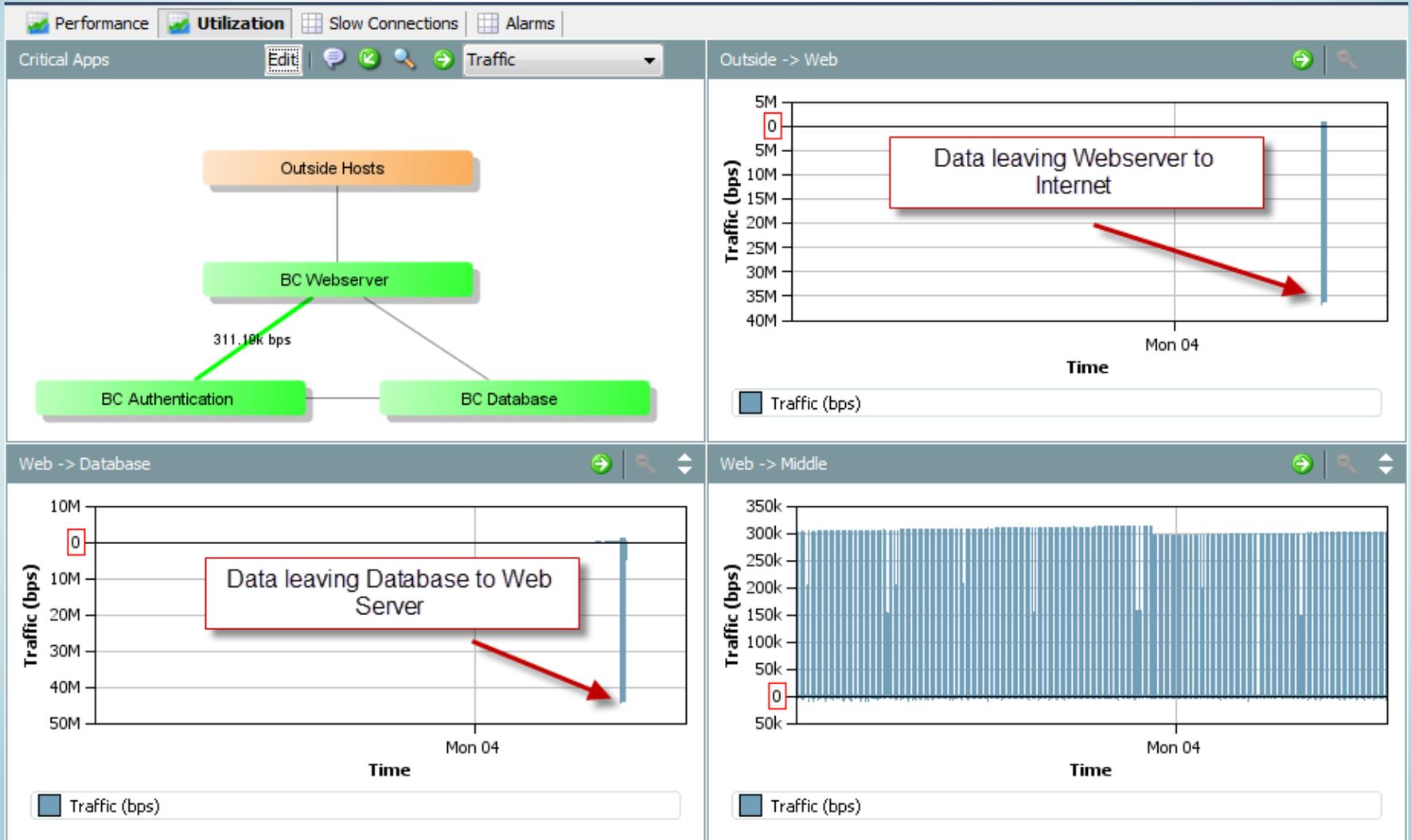


Another host showing a reverse shell

# SQL Injection



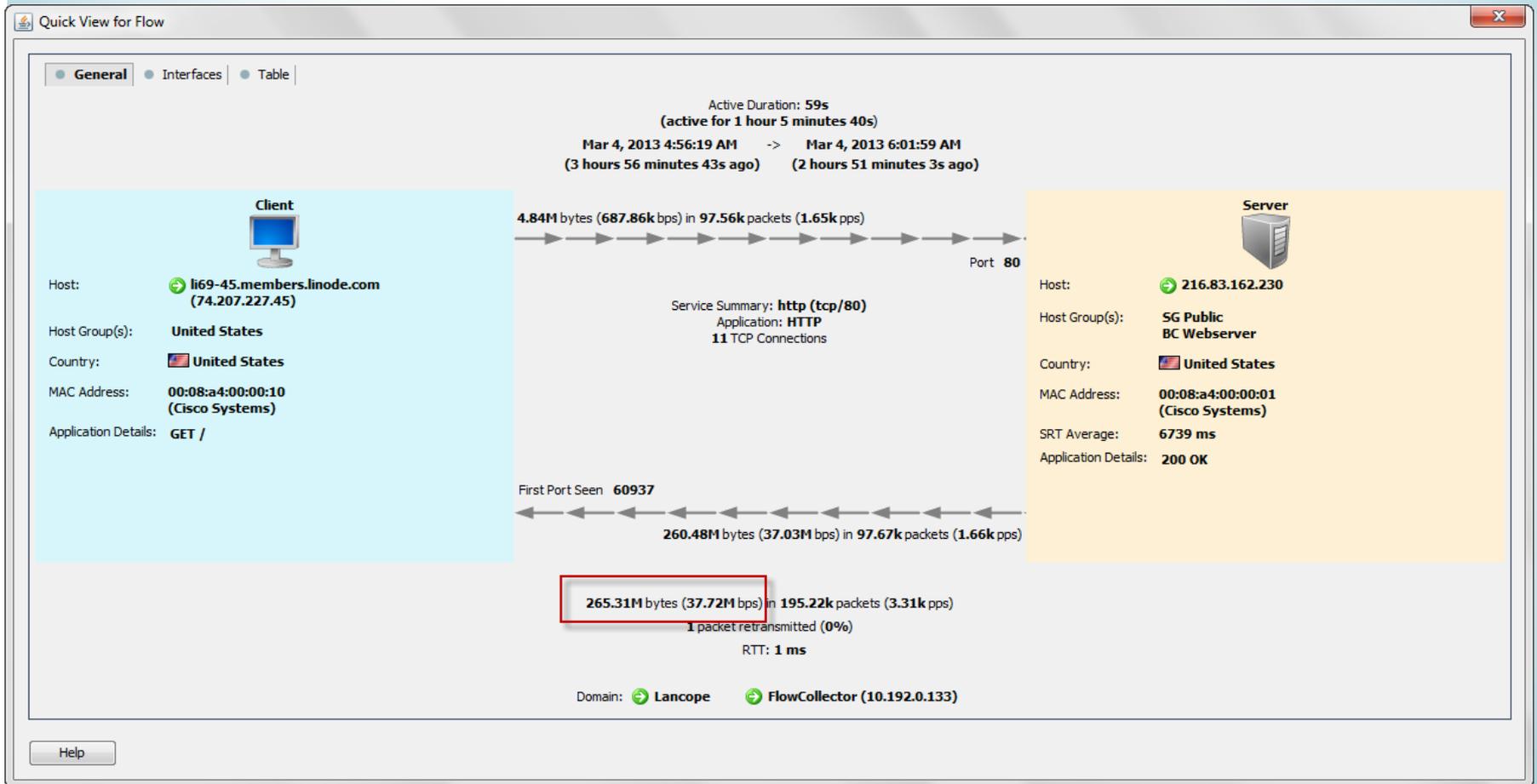
Large data transfer from your web server to an outside host was detected



# SQL Injection



Where did the data go?



# SQL Injection



Look for suspicious activity targeting the web server and your DMZ

Filter Domain : Lancope Time : Today  
Host : li69-45.members.linode.com (74.207.227.45)

Identification Alarms Security **CI Events** Top Active Flows Identity, DHCP & Host Notes Exporter Interfaces

Host is Source of CI Events (High CI) - 25 records

Start Active Time	Last Active Time	Target Host Groups	Target Host	Concer...	CI Events
Mar 4, 2013 4:55:57 AM (3 hours 59 minutes 16s ago)	Mar 4, 2013 5:05:14 AM (3 hours 49 minutes 59s ago)	United States	216.83.162.0/24	1,785,588	Ping_Scan(2560), Addr_Scan/tcp-80(492), Addr_Scan/tcp-443(520), Addr_Scan/tcp-8080(6), Ping(10)
Mar 4, 2013 4:56:01 AM (3 hours 59 minutes 12s ago)	Mar 4, 2013 5:16:36 AM (3 hours 38 minutes 37s ago)	SG Public, BC Webserver	216.83.162.230	122,669	Bad_Flag_SYN_FIN-80(200), Bad_Flag_ACK-80(40), Bad_Flag_ACK-443(40), Bad_Flag_ACK-8080(70), Bad_Flag_NoFlg-80(220), Bad_Flag_NoFlg-443(20), Bad_Flag_NoFlg-8080(20), Reset/tcp-8080(1), Timeout/tcp-8080(1), ICMP_Port_Unreach-31233(5), ICMP_Port_Unreach-36977(5), ICMP_Port_Unreach-39977(5), ICMP_Port_Unreach-41448(5), ICMP_Port_Unreach-42605(5), Ping(5)
Mar 4, 2013 5:00:00 AM (3 hours 55 minutes 13s ago)	Mar 4, 2013 5:05:00 AM (3 hours 50 minutes 13s ago)		Multiple Hosts	2,672	ICMP_Flood(2)
Mar 4, 2013 4:55:58 AM	Mar 4, 2013 5:06:41 AM	United States	216.83.162.1	2,041	Bad_Flag_ACK-80(10),

Pre-SQLi suspicious activity connected with recon

# Data Theft



One of your users has uploaded a large amount of data to the internet.

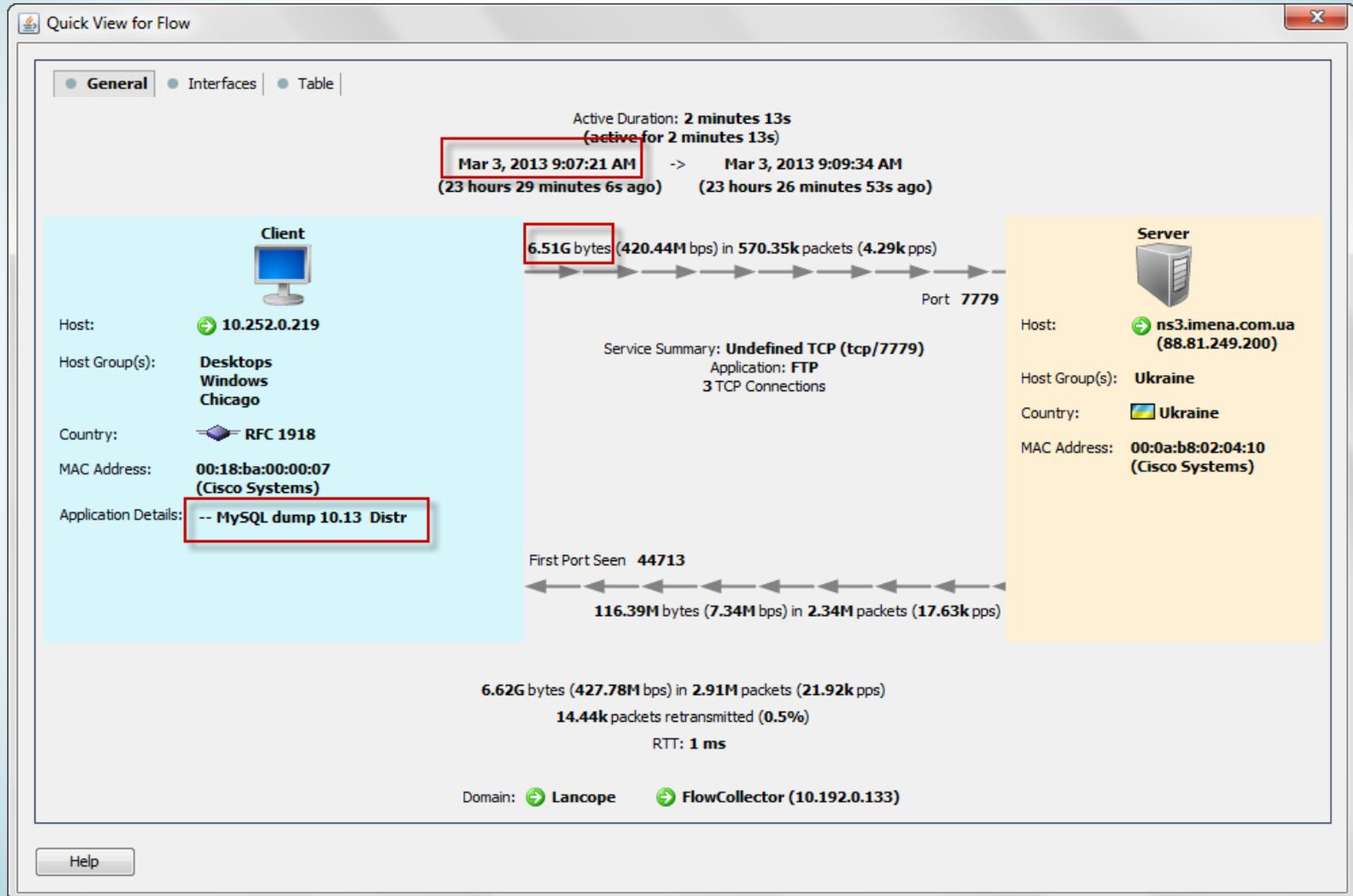
## Beron's abnormal disclosure

1	2	Policy	Start Active T...	Alarm	Source	Source Host Gr...	Source U...	Target	Target H...	Details
		Compliance Hosts	Mar 3, 2013 7:35:00 AM (1 day 1 hour ago)	Suspect Data Loss	10.210.7.38	Control Servers, Windows	lucy	Multiple Hosts		Observed 2.41G bytes. Policy maximum allows up to 1k bytes.
		Inside Hosts	Mar 3, 2013 9:15:00 AM (23 hours 20 minutes 48s ago)	Suspect Data Loss	10.252.0.219	Desktops, Windows, Chicago	beron	Multiple Hosts		Observed 8.28G bytes. Policy maximum allows up to 500M bytes.

Abnormal Data Upload



## What did Beron send? Who received it?





## Where could have Beron gotten the data?

Filter Domain : Lancope Direction : Total  
Client Host : 10.252.0.219 Time : Last 1 day  
Server Host Group : Inside Hosts

Top Peers - 2 records

	% of Bytes	Peer	Peer Host Groups	Peer Role	Average Traffic (b...)	Bytes	Flows	Hosts	Peer Bytes Ratio
1	10...	10.252.0.10	BC Database, Chicago	Server	114.68M	10.41G	1	1	98.18%
	10...	Total (1)		Server	114.68M	10.41G	1	1	98.18%



Quick View for Flow

General | Interfaces | Table

Active Duration: **11 minutes 14s**  
(~~active for 11 minutes 14s~~)

**Mar 3, 2013 8:55:57 AM** -> **Mar 3, 2013 9:07:11 AM**  
(23 hours 42 minutes 24s ago) (23 hours 31 minutes 10s ago)

Client	Server
Host: 10.252.0.219	Host: 10.252.0.10
Host Group(s): Desktops Windows Chicago	Host Group(s): BC Database Chicago
Country: RFC 1918	Country: RFC 1918
MAC Address: 00:08:a4:00:00:09 (Cisco Systems)	MAC Address: 00:05:dc:1d:10:00 (Cisco Systems, Inc.)
Application Details: !	Application Details: 4.....5.1.61!..WKP2FL*,...

194.25M bytes (2.42M bps) in 3.92M pack  
Port 3306

Service Summary: **mysql (tcp/3306)**  
Application: SQL  
15 TCP Connections

First Port Seen 46823

130.3M bps in 1.99M packets (2.95k pps)

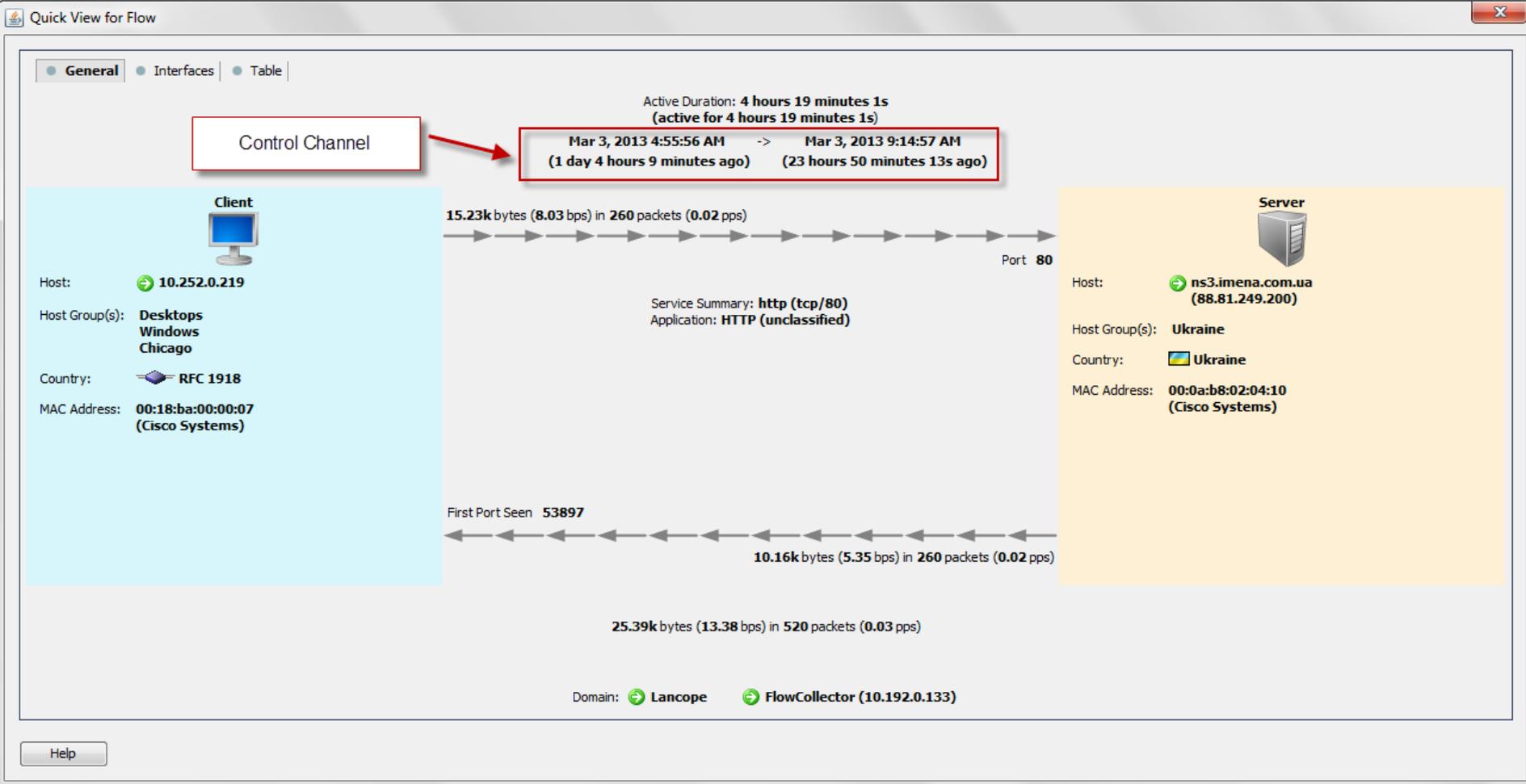
10.41G bytes (132.71M bps) in 5.9M packets (8.76k pps)  
12 packets retransmitted (0%)  
RTT: 1 ms

Domain: Lancope FlowCollector (10.192.0.133)

Help



## Why did Beron do it?





- **Web**

[www.lancope.com](http://www.lancope.com) (Company)

- **Twitter**

[@Lancope](https://twitter.com/Lancope) (Company)

[@netflowninjas](https://twitter.com/netflowninjas) (Company Blog)

- **John Pierce**

*Sr. Security Researcher, Lancope*

[jpierce@lancope.com](mailto:jpierce@lancope.com)

